Legal Tech: Issues of Ethics and Compliance

CEJ
COMPLIANCE ELLIANCE JOURNAL

Content Curators:
Michele DeStefano (University of Miami School of Law)
Dr. Hendrik Schneider (University of Leipzig Faculty of Law)

ISSN 2365-3353
Volume 4 • Number 1
Spring 2018

Compliance Elliance Journal (CEJ)
Volume 4, Number 1, 2018
ISSN: 2365-3353
This version appears in print and online. CEJ is published twice per year, in spring and fall.

Title: Legal Tech: Issues of Ethics and Compliance

Website: www.cej-online.com

Email: info@cej-online.com

Address:
Taunusstrasse 7
65183 Wiesbaden, Germany

Telephone: +49 0341 / 97 35 220

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

Legal Tech: Issues of Ethics and Compliance

TABLE OF CONTENTS

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

EDITORIAL

LEGAL TECH: ISSUES OF ETHICS AND COMPLIANCE

We are pleased to present you a new edition of the Compliance Elliance Journal (CEJ).

This edition will focus on questions regarding Legal Tech and Compliance.
The ongoing digitization concerns almost every aspect of our daily lives. As a result, many processes and transactions have been facilitated, our ways to communicate, to work and to obtain information have been changed. These developments raise not only new legal questions but do similarly affect the legal working environment and the ways legal services are provided. This edition of CEJ will examine which new opportunities so called "Legal Tech" can offer and what kind of risks the recent trends may involve.

The first two articles deal with new opportunities so called "smart contracts" can provide. Firstly Erick Gavin examines how the system of Blockchain can not only serve as a cryptocurrency but equally as basis for self executing smart contracts in his essay "Is a Trustless System an Ethical System?". Smart contracts are not only interesting with regard on questions of fraud resistance but similarly on equity aspects. As they may strengthen the position of the inferior part of a contract.
Martin Fries writes on the role compliance plays, in the field of private law. In his article "Private Law Compliance through Smart Contracts?" he examines potential implications for private law if smart contracts become to be increasingly established in the field. He argues that such a development would enable customers to enforce their rights more easily and thus make consumer protection more effective.

Similar improvements can be expected from the use of legal chatbots: In "Legal Chatbots – Characteristics, Recent Developments and Ethical Implications" Martin Bartenberger, Sven Galla and Alexander Kosak focus on the idea of support by legal chatbots and introduce the first legal chatbot used on the German legal market. The authors discuss how chatbots can improve access to justice for everyone and facilitate the communication between lawyers and their clients, often characterized by a knowledge gap between both parties and an unintelligible technical language. Critically, however ethical aspects and challenges of the recent and possible future developments require precise examination.

As the subject of digitization cannot be considered in full without paying attention to questions regarding cyber security and data protection, the authors of the article "Overcoming the Security Quagmire: Behavioural Science and Modern Technology hold the Key to solving the Complex Issue of Law Firm Cyber Security" analyze the digitization of legal professions in light of the above mentioned issue areas.David O'Donovan and Alexandra Marshakova understand human flaws as the weakest spots for cyber protection.

Law firms in particular are at risk and require approaches to improve and ensure data protection and establish functioning cyber defence systems.

The legal restrictions legal tech start-ups face in Germany will be assessed by Frank Remmertz. His essay “Scopes and Limits of the German Legal Services Act for Legal Tech Providers” examines the progress of legal service regulation in Germany in comparison to other jurisdictions. The author emphasizes on how crucial it is for legal tech entrepreneurs to get an understanding and knowledge of the issues concerning legal service regulation to detect as early as possible potential obstacles to avoid conflicts and problems later on.

Lastly Martina Orrù provides an outlook for the next issue of CEJ which will focus on the subject of E-Health and Telemedicine. She reports on the conference "Compliance Management in Institutions of the Healthcare System" which took place in Bielefeld, Germany in March 2018. The conference dealt with pressing questions regarding compliance in healthcare, in particular in light of the introduction of criminal offences of corruption and bribery in the healthcare system to the German criminal code in 2016.

We hope you enjoy our spring edition!

With our best regards,

Michele DeStefano & Dr. Hendrik Schneider
Founder and Content Curators of CEJ

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

IS A TRUSTLESS SYSTEM AN ETHICAL SYSTEM?

Erick Gavin

AUTHOR

Erick Gavin is a student at the University of Miami School of Law finishing up his last year. Throughout his time in law school Erick Gavin has invested a lot of time into the Miami Entrepreneurship and Innovation Ecosystem. This has sparked his interest in working more with technology and design in business, specifically in Information Architecture. As he matriculates from law school he will deepen his skills with data analysis, data visualization, and design in digital environments that will continue to help him grow professionally.

ABSTRACT

If you have not been hiding under a rock you have heard the whispers about Bitcoin and Blockchain, and they are going to revolutionize everything we do (or scam everyone into debt at the very least). One very interesting part of this technology is the idea of Smart Contracts – programs that automate the process of an agreement between two entities essentially to circumvent aspects traditional problems with executing and enforcing said contract. While in the legal community Smart Contracts have been talked about at length about whether they can truly succeed in replacing certain functions of the legal system, one question that has yet to be asked is if they are a viable substitute are many people immediately placed in a detrimental or even harmful situation. The pervasiveness of Blockchain and Smart Contracts will not affect everyone in our society equally and that must be taken into consideration.

TABLE OF CONTENTS

I. INTRO-BLOCKCHAIN AND SMART CONTRACTS

Technology has always been a driving force in our society simultaneously enriching our lives while adding a steep level of complexity to many aspects of our lives. While this trend has always been a steady constant there have been tipping points that have marked turning points in the growth of our technology. The Industrial Revolution, the Internet, and now there is the potential for another technology to have a substantial effect on our lives once again – Blockchain. Blockchain is short is a decentralized ledger that records information on a chain of blocks that are constantly growing and immutable – unable to be changed.[1] One way to think about a Blockchain is to imagine you are building a group of libraries. Each day you create a new section of books to be added to one of your libraries. Some days by author and others by content, but at the end of each day a "block" of records is created with whatever new books you have brought into the library that day. That block contains all the information about the books that were brought in that day from the time they brought in to the author that wrote them. After each day these blocks "chain" together chronologically, making a running record of "book blocks" that cannot be changed. When you bring in new books or take old books out the record of books in the past blocks remain the same, but the changes are recorded in the new block on the day the changes were made. All of these additions and changes are reflected in every single one of your libraries at the same time once they are "validated" by operators, miners in real life, within that particular Blockchain. There is a lot I am leaving out of this example, but the main thing to grasp is the immutability and the decentralized nature of the network. Blockchain has the potential to move our society forward in many positive directions just as its predecessors. Efficient transactions, automation of agreements, and visibility of records across a network speak to just a few of the benefits that Blockchain is improving upon processes currently present. In the same vain as its predecessors Blockchain is bringing to mind different issues that will not only effect the business field but the legal industry.

Large Businesses are starting to see the commercial viability of Blockchain and are testing its capabilities for future use.[2] What is important to note here is that everyday people and consumers will more likely than not get their first taste of Blockchain from the enterprise level.[3] Enterprise level technology will have clear benefits for business operations with the legal field nicely creating regulation around the adaptation of Blockchain technology, but

---

1 Ameer Rosic, *What is Blockchain Technology?*, Blockgeeks (Apr. 04, 2018, 11:13 AM), https://blockgeeks.com/guides/what-is-blockchain-technology/.

2 Bloomberg, *Blockchain is Pumping New Life into Old School Companies like IBM and Visa*, Fortune (Apr. 04, 2018, 11:17 AM), http://fortune.com/2017/12/26/blockchain-tech-companies-ibm/.

3 Hyperledger, *What is Hyperledger? Brian Behlendorf Executive Director Of The Hyperledger Project Explains*, The Linux Foundation Projects (Apr. 04, 2018, 11:17 AM), https://www.hyperledger.org/news/2017/10/02/10-2-17-cryptocoinnews-what-is-hyperledger-brian-behlendorf-executive-director-of-the-hyperledger-project-explains.

that it is not clear that his will occur in the same way with individuals and consumers affected by these business field improvements. One of these unclear advances are the improvement of Smart Contracts, which are automated agreements that can be enforced either by a court or some execution of computer code.[4] The ability to enforce an agreement beyond the court creates an interesting dynamic between the two parties stated within the agreement.

In this paper one will be focusing on Blockchain in general while also narrowing in on Smart Contracts developments of Blockchain that have could have the biggest implications on the legal field. Smart Contracts have been amplified in their use by Blockchain because they can now be deployed in many different technologies given the decentralized nature of the Blockchain, mainly taking advantage of the cryptographic security insured by the Blockchain.[5] Blockchain technology will oddly enough place consumers and everyday people in a type of a paradox where they have more access from a trustless democratized system while the complexity of that same system can be used to the advantage of those who better understand it and have set up the system more for the benefit of those entities. In technology one must always consider the residual impacts of advances on different demographics, much like one uses Race and Class to define sections of society that are negatively impacted by certain policies within the law. Contracts as a field of law already covers these inequities and it is interesting to see how Smart Contracts will affect vulnerable groups. Not withstanding the hype around Crypto Currencies Blockchain is here to stay and the sooner we can identify possible problems the better the legal field can pivot to properly cover them to protect people.

II. CONSUMER POWER?

When I dove head first into Blockchain and Smart Contracts the first thing that really excited me was the idea of a decentralized system that put everyone on the same playing field as user of the system. Unfortunately, I was reminded that power and control resides in who designs the system that even a system like this can be used to distort that equal balance of power. Blockchain by its nature is meant to deter this, but is it still possible to alter this foundational aspect of Blockchain if a company wanted?

The main application that people see Blockchain in currently is through the Crypto Currency and the investment potential of using these tokens as assets, SEC does not currently treat them as securities in most circumstances.[6] Although these are financial Blockchains

4 C.D. Clack, V.A Bakshi & L. Braine, *Smart Contract Templates: foundations, design landscape, and research directions*, ArXiv e-prints (Apr. 04, 2018, 11:24 AM), https://arxiv.org/abs/1608.00771.

5 Reggie O'Shields, *Smart Contracts: Legal Agreements for the Blockchain*, 21, BANKING INSTITUTE JOURNAL, 177 (2017).

6 Jay Clayton, *SEC Statement on Cryptocurrencies and Initial Coin Offerings*, U.S. Securities and Exchange Commission (Apr. 04, 2018, 11:33 AM), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

focused on shares of tokens in an Initial Coin Offering one can see the different economic aspects at play when negotiating for a plan as we did before. Here for example, we can return to healthcare plans for individuals with the different healthcare providers. In many ways this could be an improvement to the current system since it is allowing consumers to automate the manner in which they are receiving healthcare (such as their plans being updated as their change in conditions are recorded by their doctors). Looking at the system itself the healthcare providers would at the least have a say in how most of the Blockchain is designed if not practically design it themselves to favor the companies. A dynamic that resembled working in parallel to maintain "reasonable prices" as they do now just being played out digitally on the Blockchain in an even more complex manner.

While one should be confident that these transactions will be done in a more efficient manner one must always ask at what cost. My fear would be not that one would not eventually be able to mitigate these things, but that the law will remain reactionary in the same way that the SEC has been with Crypto Currencies. Understanding how Blockchain will either improve or alter that should be a policy concern for those who will not be able to stay abreast on intricate matters of this nature. Algorithms now already fall prey to the intricacies of human interaction.[7] It is imperative that if these digital systems will start to command more transactions and situations in the outside world that regulations guide this evolution for those who do not have the power to understand it themselves.

III. A SOCIETY UNAWARE

One large problem that the Internet intensified was the use of adhesive contracts as well as multiplied the amount of people who didn't fully investigate the contracts they were signing.[8] This problem was partly curtailed with the enacting of the UETA because of the regulation around electronically entering into and signing a contract.[9] Smart contracts add a new another layer to this problem because it is not particularly clear exactly when someone may be getting into a transaction. A highly used example is the purchase of a vehicle by way of a loan. Once the first party comes into to buy the car they must set conditions on which the car can be bought and remain in the owners possession through payment of the loan. Smart contracts modify this relationship by giving wider ability to the dealership/loan owner to enforce non-payments on a loan by stopping the car's use once payments on the car are stopped. This example shows the benefits of Smart Contracts in a very defined way. A company should have the ability to enforce their contract in a more direct manner, as directly stopping use of the car is an efficient solution to a breach of contract. This example is fairly black and white, but transactions are not always

7 Christian Sandvig, *When the Algorithm Itself Is a Racist: Diagnosing Ethical Harm in the Basic Components of Software,* 10, INTERNATIONAL JOURNAL OF COMMUNICATION (2016).

8 Andrew A. Schwartz, *Consumer Contract Exchanges and the Problem of Adhesion*, 28 (2), YALE JOURNAL ON REGULATION (2011)

9 Uniform Electronic Transactions Act 1999 (UETA) § 14, (Apr. 04, 2018, 11:46 AM), http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf.

black and white.

When relationships become more intricate and happen autonomously one could begin to move into a grey area of transactions not being clearly defined as contracts, but effectively establishing relationships with new or familiar entities in ways that one may not be readily aware of. If one thinks of the Blockchain as something in the future that will house much of our information, much like in Estonia right now where the entire government is taking the initiative to make their citizens access services through digital means, then relationships can be established with major corporations that everyday citizens will not take the time to fully investigate.[10] One can imagine a world where you are put on notice once for entering into a Blockchain system all of which can encompass a multitude of actions and interactions, and everything else is implied after that point. For example acceptance on particular Blockchain individuals could have the ability to negotiate contract prices, services like cell phone carriers or healthcare plans. The smart contracts on the Blockchain would be responsible for negotiating prices between the individual and the various companies to reach the most reasonable price. In this scenario Smart Contracts on the Blockchain are facilitating the much needed help of wading through the many available services that competing companies are offering consumers that do not normally have the knowledge and time to do this themselves. Initially entering into the Blockchain would necessitate going through a contract, but does the legal representation of that contract need to detail every aspect of the additional transactions that are bound to come and change in the future. Contracts by nature normally need to be re-negotiated because expecting both the parties to understand and foresee every kind of future interaction is very burdensome.[11] Additionally, Smart Contracts do not currently have the capability to be redeployed for modifications and this limits the type of full-scale Smart Contract automations that would be necessary to make a system of very complex magnitude run.[12]

The hope would be that moving forward there were checks at different places within these systems to give consumers the ability to change how these intricate systems were evolving has the system responded to new parameters, but it is not clear how a court will be able to level with a Smart Contract that is attempting to do all of the enforcement through the technology itself. In this current iteration this could be very problematic for people who have lower socio-economic status because they maybe pushed into programs like this being the best viable solution, but have no way to fully track how their own relationships will evolve over time with different companies that they are negotiating agreements with.

The other side of this problem is simply the lack of depth with technology that a lot of society may be forced to interact with generally. There is an ever-widening knowledge gap that everyday people have with technology in general. Most of this technology is in many

---

10 Nathan Heller, *Estonia, the Digital Republic*, The New Yorker, (Apr. 04, 2018, 11:51 AM), https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic.

11 Christopher D. Clack, Vikram A. Bakshi & Lee Braine, *Smart Contract Templates: foundations, design landscape and research directions*, eprint arXiv (Apr. 04, 2018, 11:54 AM), https://arxiv.org/abs/1608.00771.

12 Id. at 4.

ways harmless whether we understand it or not because not understanding it isn't a direct detriment to that individual's life. Technology failing doesn't mean years of problems and potentially irreversible states of being for an agreed upon relationship, but in the legal field lawyers are all too familiar with the idea of harmless agreements blowing up into large problems that cause havoc on a relationships. For very established companies these problems are mostly negligible and can be written off as part of the adoption process of a new technology or process, but people with limited resources will now have to overcome an additional hurdle beyond their limited ability to fully comprehend every transaction they enter into.

For example, one can take our car loan example again, but this time delve a little deeper into the mechanics of the hypothetical contract by adding a few parameters. Let's also say that the holder of the loan is the same bank that holds several of your loans like your home, student, and a business loan for a company you are starting. It would not be unforeseeable that the bank could package these together in a way that defaulting on one loan payment could effect your usage of the other items also tied to loans. Defaulting on that student loan payment could mean more than just effecting your credit score it could literally hamper your ability to get from place to place. This may seem to some as an extreme example but it is by no means far fetched once enforcement mechanisms are identified for many aspects of our lives. Enforcement of contract being a key benefit to corporations' use of the Blockchain makes it a viable option to disrupt aspects of our lives. This is even more damning on individuals who are not in the financial position to withstand that type of disruption. One solution might be to not sign this kind of agreement, but again this goes along with the assumption that every person is equally equipped to fully understand these types of arrangements which now have an added layer of technology that connects all these once separate functions into a single one. This also doesn't take into consideration governments' on a local and federal level using Blockchain to implement a lot of the federal services that are now desperate across many different entities and departments.[13]

Again the goal here is not to extremely pessimistic about the potential of Blockchain technology, but simply be aware of how any good system can harm people unnecessarily if those who design and maintain that system are not aware of the different effects it can have at various levels.

IV. CONCLUSION

Blockchain being a budding tool transforming how one think about various fields will be difficult to measure how it is impacting different groups within our society. This reason enough that one must be very conscious of exactly how these developments change both business to business and business to individual interactions. As excited as I am for all the

[13] Blockchain for Government, International Business Machines Corp. (Apr. 04, 2018, 11:59 AM), https://www.ibm.com/blogs/blockchain/category/blockchain-for-government/.

opportunities that Blockchain is opening up for professionals like myself I must remember that privilege plays a large roll in my excitement and all the benefits that we anticipate it will bring.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

PRIVATE LAW COMPLIANCE THROUGH SMART CONTRACTS?

Martin Fries

AUTHOR

Martin Fries is a private lecturer (Privatdozent) at the University of Munich (LMU). His research focuses on various topics around civil law, civil procedure, conflict of laws, legal ethics, and legal technology. Much of his teaching is available online at https://www.youtube.com/jurapodcast/. Martin regularly serves as a mediator in commercial and inheritance disputes.

ABSTRACT

Smart contracts allow for automated compliance with contractual rules. They derive their "smartness" from an execution software that catches the most typical defaults and responds by mechanically triggering a compensation payment or another prearranged consequence. Through this self-enforcement mode, smart contracts are able to save time and effort that is associated with more customary rights enforcement mechanisms. Now, whereas compliance with in-house rules or corporate governance standards is common today, compliance with contract law only occurs on a voluntary basis. This might, however, change if businesses should be obliged to automatically meet customer claims through smart contracts. On the basis of a sample case, this article examines the pros and cons of smart consumer contracts and carves out the most suitable applications of smart contracts as a means to ensure private law compliance.

TABLE OF CONTENTS

I. BACKGROUND: TRADITIONALLY LIMITED COMPLIANCE WITH PRIVATE LAWS

Compliance typically refers to the duty of companies to act in accordance with public law. Failure to comply is sanctioned by a civil penalty or by means of criminal law. During the last several decades, the importance and influence of compliance departments has significantly grown. At the same time, whether or not businesses choose to comply with the growing body of private law is still regarded a strategic decision rather than a straightforward legal duty. Private law is designed to be available as a state-provided system of rules for cases where conflicts of private interests cannot be otherwise resolved. Traditionally, however, the enforcement of private claims is relegated to the resolve of the very persons involved. In principle, the state does not care whether market participants eventually avail themselves of their rights. If they back off from making a claim, their opponent goes free, and the state is fine with that.

This regulatory approach gives remarkable leeway to the strategic decisions of repeat players.[1] They might voluntarily meet private law obligations as an aspect of a service strategy, but they can just as easily wait out any customer requests and count on a common aversion to bring legal action. In spite of these options, there is a strong incentive to choose the latter alternative. As market dynamics focus more on low prices rather than customer service, it becomes more difficult to stand one's ground in the market without cutting back on private law compliance.[2] This calculus notably applies in the field of consumer law, because the vast majority of consumers are extremely risk-averse and have little knowledge of their rights and no experience in enforcing them. Hence, there is a considerable threshold for consumers to take legal action.[3] Sure enough, most consumer rights are mandatory and, thus, cannot be contractually waived. However, the mandatory nature of consumer rights makes little difference in this decision paradigm, as mandatory rights are just as likely to remain unclaimed.

If claimants shy away from enforcing their rights, other market participants will sometimes step in and take on the job. The law of unfair commercial practices allows businesses to sue their rivals for injunction in cases of grossly unfair market behavior. However, competition rules are usually limited to correct the way customers are approached, whereas

---

1 A profound analysis of the advantages of repeat players compared to one-shotters is provided by Marc Galanter, *Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change*, 9 L. SOC. REV. 95, 97-114 (1974).

2 The economic concept for this kind of market dynamic is the famous market for lemons as described in George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 QUART. J. ECON. 488 (1970).

3 See, e.g., Franziska Weber & Michael Fauré, *The Interplay Between Public and Private Enforcement in European Private Law: Law and Economics Perspective*, EUROP. REV. PRIV. L 525, 533 (2015).

competitors can typically neither request proper contract performance nor demand compliance with other contractual rights of their customers.[4] In some jurisdictions, consumer organizations and trade commissions dispose over special procedural rights to bundle customer claims and enforce them collectively.[5] However, these mechanisms are actually employed in only a small fraction of possible cases, which makes them hardly more effective than the existing alternatives, namely easy-to-use court or conciliation procedures.[6] Thus, compliance with private law and with consumer rights in particular remains unalluring for most market participants. From a traditional viewpoint, this is an almost natural consequence of private law being private law. However, the more companies ignore claims out of sheer calculus, the more pressing becomes the question how private law can be rendered more meaningful for legal practice.

II. SMART CONTRACTS AS A COMPLIANCE INSTRUMENT

Only recently, a potential solution for this problem has presented itself, the development of *smart contracts*. Smart contracts attempt to facilitate rights enforcement by automating contract execution, as well as the handling of typical impairments of performance. For this purpose, contracts are translated into computer code and digitally connected to some assets of the parties. Hence, the "contract machine" automatically detects changing circumstances or events of default and takes the predetermined action.[7] Of course, this concept requires contract lawyers to design a contract that anticipates as many problematic situations as possible. Moreover, programmers are demanded to link detection mechanisms (the so-called *oracles*) to the appropriate legal consequence without creating frictions with the word and spirit of the contract.

With the growing extent of data tracks, the scope of application for smart contracts is rapidly expanding. For example, a car sharing contract could be made smart by charging the renter a contractual penalty for speeding, or by automatically locking the car if she

---

4 In Europe, the law of unfair competition is governed by the Unfair Commercial Practices Directive 2005/29/EC; see Hans-Wolfgang Micklitz, *Unfair Commercial Practices and Misleading Advertising, in* Understanding Consumer Law 61-117 (Hans-Wolfgang Micklitz, Norbert Reich & Peter Rott eds., 2009).

5 A good overview on the legal situation in Europe is provided by the contributions to WILLEM VAN BOOM & MARCO LOOS, COLLECTIVE ENFORCEMENT OF CONSUMER LAW: SECURING COMPLIANCE IN EUROPE THROUGH PRIVATE GROUP ACTION AND PUBLIC AUTHORITY INTERVENTION (2007).

6 The European Union has issued a small claims procedure through its Regulation (EC) No 861/2007, recently amended by Regulation (EU) 2015/2421. With its Directive 2013/11/EU on consumer dispute resolution, the EU switched to an out-of-court approach, obliging its Member States to provide access to free-of-cost conciliation for consumer disputes; critical assessment by Horst Eidenmüller and Martin Engel, *Against False Settlement: Designing Efficient Consumer Rights Enforcement Systems in Europe*, 29 OHIO ST. J. DISP. RESOL. 261-297 (2014).

7 See, e.g., Alexander Savelyev, *Contract law 2.0: „Smart" contracts as the beginning of the end of classic contract law*, 20 INF. & COMM. TECHNOL. L. 116, 120-121 (2017); Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305, 306, 309 (2017); Mark Giancaspro, *Is a „smart contract" really a smart idea? Insights from a legal perspective*, 33 COMP. L. & SEC. REV. 825, 826 (2017); Kevin Werbach & Nicolas Cornell, *Contracts ex machina*, 67 DUKE L. REV. 313, 330-352 (2017).

illegally drives abroad. Likewise, a mobile phone contract could be complemented by software that observes network availability and issues some sort of a lump-sum compensation if the network becomes unavailable for more than ten minutes. Another scenario could involve a lawyer working on her client's documents in a cloud who receives remuneration only for the time she is actively working in the cloud database. The key advantage of a smart contract in these cases is that the parties to a contract are automatically forced to comply with their contractual duties. To put it in legal Latin: Pacta non modo sunt *servanda* sed etiam sunt *servata*.

The sixty-four dollar question, however, is: What incentive is there for any contracting party to attach a self-enforcement mechanism to a contract? Here, two cases have to be distinguished. On the one hand, where two contractors meet at eye level and could both be subject to automatic enforcement, there might be a common interest in contract reliability that leads both parties to agree to a smart contract. On the other hand, where there is a considerable power imbalance between both parties, like in consumer contracts, there is little reason for the mightier part to agree to a self-enforcing compliance system. This is exactly the very reason why many companies hesitate to meet civil claims today. Thus, the only way to change their calculus would be a law requiring companies to make use of smart contracts when doing business with consumers. This seems to be inconsistent with the nature of private law, to wit, a law that is not enforced by the state. However, at least in Germany, the government currently considers to do just that: encourage or even compel companies to use smart contracts in an effort to make the enforcement of consumer rights more effective.[8]

III. SAMPLE CASE: A SMART RAILWAY TRANSPORT CONTRACT

How could such a private law compliance mechanism be applied in practice? The parliamentary group of one of the political parties that formed the current German government offers two concrete examples. In their view, smart contracts could be used to facilitate compensation claims for flight or railway transport contracts.[9]

Thus, imagine a train carrying 100 passengers from Munich to Berlin for 100 € per ticket, the regular travel time being 4 hours. If this train is one hour late, Art. 17(1) (a) of the European Regulation No 1371/2007 on rail passengers' rights and obligations grants passengers a refund of 25% of the ticket price. If usually 10% of all trains are delayed for one hour or more[10] and 10% of all passengers take the trouble to claim their refund, the railway operator will set aside 0.25% of his turnover for satisfying these claims. Now, as soon as

8 For further details see Martin Fries, *Smart consumer contracts: The end of civil procedure?,* Oxford Business Law Blog (Mar. 29, 2018, 11:18 AM), https://www.law.ox.ac.uk/business-law-blog/blog/2018/03/smart-consumer-contracts-end-civil-procedure.

9 See the explanation at (Mar. 05, 2018, 09:40 AM), https://www.spdfraktion.de/themen/verbraucherinnen-verbraucher.

10 Delays of two hours or more result in a refund of 50% of the ticket price. To simplify matters, this is not taken into calculation here.

the respective transport contract is connected to smart enforcement software, the enforcement ratio will bounce up to almost 100%. This will make the railway operator increase the provisions from 0.25% to 2.5% of the ticket price, leading ceteris paribus to a general price increase of roughly 2%.

A rise in prices in this range will be perceptible and decision-relevant only for few customers. As a matter of fact, this finding considerably changes as soon as the compensation amount increases or is also triggered by minor delays. If, for example, the railway operator had to pay every passenger 50 cents for every minute of delay, the loss of revenue would considerably increase, and the consequential price increase would be quite perceivable. If the average long-distance train is 10 minutes late and the train operator is required to refund 5 €, on average, to every customer, ticket prices would go up respectively. Given this scenario, one might wonder about the advantages of such a system over a world without any delay compensations. Is granting a refund to a customer that she ends up paying for through increased ticket prices a better world.

IV. A CONTRIBUTION TO MARKET EFFICIENCY

The main reason for an appropriate compensation of damages in general and transportation delays in particular is fair competition.[11] In a price-oriented market economy, market participants expect the cost of a product or service to reflect a good or service that is free of impairments. If customers pay the full price, but receive only faulty contract performance without a compensation, their product choice and, thus, the functioning of the market will be flawed. Companies will anticipate this mechanism and often interpret it as a complimentary ticket to defer necessary investments in the quality and reliability of products and services.

Of course, those misguided incentives for businesses will sometimes be alleviated by disappointed customers sharing their experience with others and thereby lowering the market expectation of product quality. For example, a frequent rail traveler will soon get a feel for the delay she can expect when traveling by train and, if need be, switch to other means of transportation like planes, buses, or rental cars. However, this mechanism only works in markets where there is considerable competition and with either frequent deal iteration or reliable information exchange between customers, e.g., within the framework of a quality rating system provided by a trading platform. In a market without these features, damage compensation makes an important contribution to properly functioning competition and, thus, market efficiency. This expectation, however, is based on several requirements that a compensation scheme has to meet in order to actually make the market better off.

---

11 This is, of course, a very condensed statement that is not meant to slur the extensive literature on the purposes of compensatory damages; see, e.g., Steven Shavell, *Damages Measures for Breach of Contract*, 11 BELL J. ECON. 466-490 (1980); RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 128-140 (9. ed. 2014) with further references.

V. PRECONDITIONS TO AN EFFECTIVE SMART COMPENSATION SCHEME

The best enforcement mechanism cannot achieve a better result than the one determined in the underlying substantive law. The special challenge for smart enforcement mechanisms is their need for simple laws whose legal elements can be easily assessed. Lump-sum compensation laws, like the airline passenger rights laid down in Art. 7 of the European Regulation No 261/2004, are a good example for fairly automatable rules. At the same time, such a simplifying regulatory technique comes at the expense of the merits of every particular case where the appropriate compensation might not only vary, but also be difficult to quantify.

Another aspect to bear in mind is the coding design of the compliance software that is used to cure typical events of default by issuing a money transfer, locking or unlocking the object of agreement, or the like. The software needs to match the underlying contract as far as possible, because if there is any doubt about the default, the contract itself has the final say.[12] However, experience tells us that algorithms always come along with programming errors, be it because of inadvertence or by intention of one party without genuine willingness to comply. This calls for an algorithm check by some neutral agency as long as the enforcement mechanism is not set up on neutral ground like on a blockchain. In the case of passenger rights, this algorithm check could be performed by a government agency like the British Office of Rail and Road, the French Autorité de Régulation des Activités Ferroviaires, or the German Bundesnetzagentur.

Last but not least, it is worth mentioning that a smart compensation scheme can lead to a distortion of competition if some competitors are obliged and others are not. Thus, if a government decides to impose civil law compliance duties only on certain companies while leaving others unregulated, this decision should be based on well-founded criteria. Such criteria could be a factual opacity of product quality, or a monopolistic situation that makes a business insensitive towards customer feedback. Both criteria might indeed most likely be met in the field of passenger transportation as there is low competition on many national and international routes, and even experienced customers can only rarely assess the probability of an on-time arrival.

VI. CONCLUSION

Smart contracts combine legal obligations with a compliance mechanism. A conventional contract is enhanced with software that automatically issues legal consequences once a pre-specified trigger event is detected. Quite recently, discussions have been initiated about using smart contracts as a means to achieve compliance with private consumer law. It is debatable whether a public law obligation that forces companies to add an automated enforcement component to their consumer contracts goes well with the traditional concept of private rights being dependent on the proactive behavior of the claimant. Anyway,

12 Martin Fries, *Smart Contracts: Brauchen schlaue Verträge noch Anwälte?,* ANWBL 86, 87 (2018).

if the use of smart contracts shall be imposed on businesses, the analysis has shown that this approach will be most useful in monopolistic industries where the market does not provide other effective mechanisms to ensure the quality of a product or service.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

LEGAL CHATBOTS – CHARACERISTICS, RECENT DEVELOPMENTS AND ETHICAL IMPLICATIONS

Martin Bartenberger, Sven Galla & Alexander Kosak

AUTHORS

Martin Bartenberger is the co-founder and CTO of the technology-driven law firm RATIS located in Passau, Germany. A political scientist by training he holds a masters degree from the University of Vienna and a PhD from Leiden University. He has taught at the University of Vienna and the Vienna University of Economics and Business and has worked as a programmer and research manager before co-founding RATIS. He is the lead developer of RATISBOT, Germany's first legal chatbot.

Sven Galla is the co-founder and CEO of the technology-driven law firm RATIS located in Passau, Germany. He studied law at the University of Passau and was a research assistant at the Institute of Civil Law, Civil Procedure and Private International Law. Before founding RATIS he was founding partner at a regional law firm where he practiced law for over ten years.

Alexander Kosak, former scholarship holder of the "Deutschlandstipendium", is a paralegal at the technology-driven law firm RATIS located in Passau, Germany. He studied law at the University of Passau until 2018 and finished his studies with the first state examination. Since April 2018 he continues his education as a junior lawyer.

ABSTRACT

This article introduces the idea of legal chatbots and how legal chatbots might affect the legal market in the near future. We define chatbots as computer programs that automatically chat with users and assess their potential for legal consultation. We identify four potential strengths of legal chatbots: providing access to justice, serving as contact points for customers, reducing the knowledge gap between lawyer and client and automatically generating documents and taking further actions. In the concluding section we briefly discuss ethical aspects of legal chatbots and possible future developments.

TABLE OF CONTENTS

I. WHAT ARE CHATBOTS?

Living in the 21st century it is sometimes hard to keep up with the newest technical terms and buzzwords. Really grasping the deep meaning and the consequences of terms such as „cloud computing", „semantic web" or „artificial intelligence" is hard even for technical experts. Luckily „chatbot" – the technical concept we are discussing in this article – is simple to understand. Chatbots are computer programs that automatically chat with users, either via text (think of chat platforms such as WhatsApp) or via natural speech (think of Amazon's Alexa for instance). The user can ask the chatbot questions („Will it be raining tomorrow?") and gets a (hopefully) useful answer („Tomorrow the weather will be sunny and you can leave your umbrella at home"). This is the essence of chatbots.

The strength of chatbots is to create a form of communication that resembles a natural conversation between humans. The first chatbots were already created back in the 1960s. Joseph Weizenbaum's psychotherapist chatbot ELIZA is usually labeled as the first chatbot ever created[1]. On a very basic level ELIZA emulated the questions and answers of a psychotherapist and created the illusion for users that they were communicating with a real therapist. This conversational dialogue between user and computer program is the key characteristic of chatbots till this day and one of their main advantages.

Chatbots are now widely regarded as the successor of „apps"[2]. A few years ago apps were the latest trend and smartphone users installed a large number of apps on their phones for very different tasks. But the problem about apps is that many of them offer little additional functionality compared to the vendor's website. Studies quickly found that many of the installed apps were therefore almost never used after they were installed.[3]

A second disadvantage of apps is the fact that they are splitting communication channels. To communicate with company A a user has to install app A and learn how it works. To communicate with company B the user has to install an additional app and find out how

---

1 Joseph Weizenbaum, *ELIZA—a computer program for the study of natural language communication between man and machine*, 9, COMMUNICATIONS OF THE ACM, 36–45 (1966); For a brief historical overview see: Collette Curry & James O'Shea, *The implementation of a storytelling chatbot*, Paper presented at the 5th KES International Conference, KES-AMSTA 2011, Manchester, UK (2011).

2 See e.g. Marco della Cava, *Microsoft CEO Nadella: 'Bots are the new apps'*, USA Today (Apr. 04, 2018, 01:30 PM), https://www.usatoday.com/story/tech/news/2016/03/30/microsof-ceo-nadella-bots-new-apps/82431672/ and *Bots, the next frontier*, The Economist (Apr. 04, 2018, 01:32 PM), https://www.economist.com/news/business-and-finance/21696477-market-apps-maturing-now-one-text-based-services-or-chatbots-looks-poised.

3 Sarah Perez, *Nearly 1 in 4 people abandon mobile apps after only one use*, TechCrunch Today (Apr. 04, 2018, 01:33 PM), https://techcrunch.com/2016/05/31/nearly-1-in-4-people-abandon-mobile-apps-after-only-one-use/ and Kimberlee Morrison, *1 in 5 Apps Are Used Once — and Never Used Again*, AdWeek (Apr. 04, 2018, 01:33 PM), http://www.adweek.com/digital/1-5-apps-used-never-used-infographic/.

to use it. Chatbots solve this problem by creating an integrated and intuitive communication channel. In other words: most users know how to interact with a chatbot instantaneously because the communication style resembles human conversations.

Today chatbots are already used by many different companies in many different areas. They can be used via the company's website, Facebook Messenger, WhatsApp, Amazon's Alexa or similar platforms. Chatbots are especially deployed for customer support where they help customers with simple tasks and regularly asked questions.[4]

II. THE POTENTIAL OF LEGAL CHATBOTS

While widely used in many different fields already the usage of chatbots for legal consultation has been very limited so far. The most prominent „legal chatbot" is named DoNotPay and has helped people in the U.S. and in the U.K. to overturn 160,000 parking fines[5]. Yet, we believe that this is just the beginning and see a great potential for legal chatbots not only in the U.S. and the U.K. but also in Germany. We identify four main potentials of legal chatbots that might promote their dissemination.

A. Chatbots can improve access to justice

The European Union Agency for Fundamental Rights (FRA) has found that access to justice is still a problem in several EU Member States. As FRA argues, this „is due to several factors, including a lack of rights awareness and poor knowledge about the tools that are available to access justice"[6]. We argue that legal chatbots might be able to improve this situation by providing accessible and easy-to-use tools for citizens who wouldn't learn about their rights otherwise. Similar to chatbots in general customer service legal chatbots could thus serve as initial entrance points that provide basic information and guidance. For more specific advice and analysis a legal chatbot could then bring in a human lawyer for advanced support.

B. First Contact

The first dialogues between lawyers and their clients are often structured in similar ways. To gain a quick understanding of a situation lawyers routinely go through a pre-determined set of questions. This is a task that could be easily fulfilled by chatbots. From our

4 If the chatbot is unable to help the customer it often offers to bring in a human customer agent for further support.

5 Elena Cresci, *Chatbot that overturned 160,000 parking fines now helping refugees claim asylum*, The Guardian (Apr. 04, 2018, 01:33 PM), https://www.theguardian.com/technology/2017/mar/06/chatbot-donotpay-refugees-claim-asylum-legal-aid.

6 Access to justice, European Union Agency for Fundamental Rights (Apr. 04, 2018, 01:33 PM), http://fra.europa.eu/en/theme/access-justice.

perspective chatbots are therefore perfectly suited to serve as entry points for the communication with clients. In a first dialogue chatbots can collect basic information about a client and her case. This information can then be forwarded to a lawyer who is able to gain a first understanding about a case before she calls the client directly.

C Tracking in the knowledge gap

The dialogue between lawyer and client is the prevalent form of a lawyer's daily communication. Yet, linguist studies have shown how effective communication is often hindered by the knowledge gap between the lawyer and the client. In other words, clients often find it difficult to understand the technical language of lawyers while lawyers routinely fail to grasp the needs and problems of their clients.[7] We argue that chatbots could help to bridge this gap between lawyers and their clients and enable more effective communication. Compared to a conversation with a lawyer, time pressure is significantly reduced when communicating with a chatbot. While communicating with a chatbot clients have much more time to understand complex legal concepts and might even take a short break in the chatbot dialogue to inquire about certain aspects before they continue. Clients might also feel less intimitated to ask specific questions and query about aspects they don't understand.

D Generating documents and taking further actions

Since chatbots collect basic information from their users they can use this information to automatically generate certain documents as well. The chatbot of RATIS for instance provides a dialogue for users who were affected by a flight delay. After asking a set of questions about the flight delay the chatbot determines if the user is eligible to receive a financial compensation. If this is the case and the user agrees the chatbot automatically generates a letter to the respective airline claiming this compensation. This letter is send immediately and without any cost for the user.

III. RECENT DEVELOPEMENTS

While legal chatbots such as DoNotPay have gained some early fame in the U.S. and the U.K. already in Germany we only saw theoretical discussions about legal chatbots until last year. Inspired by DoNotPay and others RATIS released RATISBOT, the first German legal chatbot, last summer.[8] When we launched RATISBOT it was able to help users in claiming compensation for flight delays. We have recently expanded the scope of RATISBOT to cover employment law and lay-offs and plan to add more topics in the future.

---

7 INA PICK, DAS ANWALTLICHE MANDANTENGESPRÄCH. LINGUISTISCHE ERGEBNISSE ZUM SPRACHLICHEN HANDELN VON ANWALT UND MANDANT (1st. ed., 2015).

8 Hendrik Wieduwilt, *Der Computeranwalt aus dem Donau Valley*, Frankfurter Allgemeine Zeitung (Apr. 04, 2018, 01:40 PM), https://ratis.de/wp-content/uploads/2017/05/FAZ-15.5.2017_Der-Computeranwalt-aus-dem-Donau-Valley.pdf.

Yet, at this stage we regard RATISBOT mainly as a proof-of-concept. RATISBOT employs some basic Artificial Intelligence techniques (mainly in the area of Natural Language Processing) but is far from using their full potential. While we believe that legal chatbots have a bright future we also think that the dissemination of this new technology will take a while. The underlying technologies need to get more mature and more sophisticated first.

Right now, the usage of many chatbots is not as convenient as it could be. Even the most sophisticated chatbots regularly fail to understand their users or are having problems with trivial small-talk situations. Additionally, end users also have to get used to the idea of talking to machines. But companies such as Amazon, Google, Apple or Microsoft are rapidly paving the way for an increased acceptance of chatbots and are constantly improving the user experience. While we believe that it will take several years till we see the widespread use of legal chatbots these developments also raise important ethical questions that need to be addressed at this early stage already. We would like to briefly discuss some of them in the concluding section.

IV. ETHICAL ASPECTS AND FUTURE DEVELOPEMENTS

Just naming companies such as Amazon or Google in the context of (legal) chatbots immediately raises the issue of privacy. We share the concern of privacy and chatbots. Yet, we believe that this is a problem that nowadays affects all digital types of client-lawyer communication as well and is not limited to chatbots. Today it is common for lawyers to electronically communicate with their clients and store their data in digital databases and files, often at remote servers or in the „cloud" (which is just a more sophisticated term for remote servers). All these forms of communication are sensible to the privacy questions. We therefore regard privacy as an issue that is not characteristic for chatbot communication and therefore do not discuss it here.[9]

A. Human-Computer interaction

An ethical aspect that affects chatbots specifically is what we would label „pretended intimacy". Assuming a high level of natural language recognition and given the conversational format of a chatbot communication it might be possible for clients to forget that they are actually communicating with a machine. This phenomenon has been described by Joseph Weizenbaum, the inventor of the first chatbot ELIZA, already: „I was startled to see how quickly and how very deeply people conversing with DOCTOR [the script

9 As a general rule-of-thumb to deal with the question of privacy in our digital times we would make the case for the following best-practice: 1. explain possible risks to users, 2. provide alternatives for users (phone, snail mail, etc.), 3. self-host your applications and data where possible.

ELIZA used] became emotionally involved with the computer and how unequivocally they anthropomorphized it".[10] We regard it as crucial for the ethical development of legal chatbots to avoid this pretended intimacy. This includes being transparent about the fact that the client is actually chatting with a machine.

From our perspective such transparency caters to an additional strength of chatbots. In fact, we would hypothesize that many people may find it easier to talk to a machine about sensitive issues than to a human lawyer. As outlined in section II, chatbots could thereby help to bridge the gap between lawyer and client by providing a first opportunity to explore and probe certain sensitive issues and receive basic legal advice for them without opening up to a human lawyer.

Consider the example of a patient's provision (Patientenverfügung) for instance. Drafting such a document involves sensitive questions regarding death, illness, the value of life and many other ethical questions. A client might feel more comfortable to explore her own positions in a conversation with a chatbot than with a human lawyer she has never met before. A well-developed chatbot could use algorithms to translate the moral positions and general attitudes of a client in a concrete draft of a patient's provision. This draft could provide the base for a more detailed conversation with a human lawyer.

B. Are chatbots taking the jobs of lawyers?

Another ethical question regarding chatbots in general concerns their effect on our worklife. Put most bluntly, the question is if chatbots are taking the jobs of lawyers (and many others)? Much ink has been spilled on the question which jobs are likely to be replaced by robots or algorithms.[11] Concerning the legal profession we find Frey and Osborne's position most sensible and realistic: „we find that paralegals and legal assistants – for which computers already substitute – in the high risk category. At the same time, lawyers, which rely on labour input from legal assistants, are in the low risk category. Thus, for the work of lawyers to be fully automated, engineering bottlenecks to creative and social intelligence will need to be overcome [...]"[12].

While lawyers themselves might not be replaced by new technologies such as chatbots, chatbots might still have a substantial effect on the legal job market and reduce the number of jobs for paralegals and legal assistants. Yet, this problem is not limited to the legal

---

10 WEIZENBAUM JOSEPH, COMPUTER POWER AND HUMAN REASON. FROM JUDGMENT TO CALCULATION 6 (1st ed., 1976).

11 For a good overview see Alan S. Blinder, How Many U.S. Jobs Might Be Offshorable?, CEPS WORKING PAPER NO. 142 (2007) and Araw Mahdawi, *What jobs will still be around in 20 years?*, The Guardian (Apr. 04, 2018, 01:49 PM), https://www.theguardian.com/us-news/2017/jun/26/jobs-future-automation-robots-skills-creative-health.

12 Carl Benedikt Frey & Michael A. Osborne, *The Future of Employment : How Susceptible are Jobs to Computerization?*, 114 TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE 254 (2017).

professions alone but challenges the fabric of our whole social system and our welfare states. Realizing this potential social disruptions, this is why many technological leaders in Silicon Valley and around the world have began to embrace a universal basic income or similar ideas to mitigate these social effects.[13]

Whatever the outcome of these developments and discussions will be we are certain that the legal market will profoundly change over the next few years. The emergence of legal chatbots is just one aspect of this broader development. We would argue that whether one appreciates these changes or not it is crucial to understand them. We hope that this article has made a small contribution in understanding the challenges ahead.

13 Jathan Sadowski, *Why Silicon Valley is embracing universal basic income*, The Guardian (Apr. 04, 2018, 01:49 PM), https://www.theguardian.com/technology/2016/jun/22/silicon-valley-universal-basic-income-y-combinator.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

OVERCOMING THE SECURITY QUAGMIRE: BEHAVIOURAL SCIENCE AND MODERN TECHNOLOGY HOLD THE KEY TO SOLVING THE COMPLEX ISSUE OF LAW FIRM CYBER SECURITY

David O'Donovan & Alexandra Marshakova

AUTHORS

David O'Donovan is a trainee lawyer with U.S. firm Orrick, Herrington & Sutcliffe LLP in their London office and is currently completing the academic stage of training. Alexandra Marshakova is an IT Project Leader with the Boston Consulting Group also in London. David and Alexandra participated together in LawWithoutWalls in 2015 and were recognised for their Project of Worth, a spearphishing training model for law firm personnel, which the pair have since incorporated in the UK as Fissure Security. David and Alexandra have spoken about aspects of law firm cyber security and organizational behaviour at IE University Madrid, University of Miami and Harvard Law School.

ABSTRACT

While all industries that handle valuable data have been subject to increasing levels of cyber attack, there is a set of inter-related factors in the law firm cyber security ecosystem that makes such firms more susceptible to attack and also serves to prevent them from taking action to counteract attack vulnerability. As a result of the inter-related external and internal factors affecting law firm cyber security, the human element of firm security infrastructure has been neglected, thereby making humans, at once law firms' greatest asset, their main cyber security weakness. [1]There has been some movement of late, and regulators and clients alike are right to demand law firms do more to improve their cyber security posture.[2] However, much of the scrutiny to which their conduct has been subjected has tended to overlook the complexities of the law firm cyber security quagmire, and unless these issues are addressed in the context of a potential solution, meaningful change is not

---

1 Russell G. Pearce & Eli Wald, *The Relational Infrastructure of Law Firm Culture and Regulation: The Exaggerated Death of Big Law*, 42 HOFSTRA L. REVIEW, 109 (2013).

2 Julie Sobowale, *Law firms must manage cybersecurity risks*, American Bar Association Journal (Mar. 29, 2018, 12:37 PM), http://www.abajournal.com/magazine/article/managing_cybersecurity_risk; See also: McNerney, Michael & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, AMERICAN UNIVERSITY LAW REVIEW 62, 1243-1272 (2013).

likely. Part 1 of this paper outlines the current threat landscape and details the integral role of human error in successful cyber breaches before turning to discuss recent cyber security incidents involving law firms. In Part 2, we analyse elements of law firm short-termism and the underregulation of law firm cyber security conduct and how these, when combined, play a key role in shaping law firm cyber security posture. Finally, in Part 3 we outline a realistic solution, incorporating principles from behavioural science and modern technological developments.

TABLE OF CONTENTS

I. PART 1 – THE CURRENT THREAT LANDSCAPE

A. Attacks on the rise

In recent years, cyber attacks have been growing in frequency, intensity and complexity. Notable examples of breaches include household names such as Equifax, Uber, Yahoo!, Sony, Netflix, JP Morgan, Target, Anthem, and Epsilon[3], as well as prominent international sports stars, politicians, members of the British monarchy and Russian oligarchy.[4] With a more diverse range of perpetrators than ever before, including (amongst others) nation states, hacktivists, and individual private contractors, and a wider variety of attacks ranging from denial-of-service to ransomware, 2017 may just be the year in which the world reached peak cyber attack. An inordinate number of breaches were recorded - some on a very public stage, particularly WannaCry and Petya - which affected government departments, international law firms and brought the UK National Health Service to a standstill. Initial reports of cyber attacks this year suggest that 2018 has continued in much the same vein, with high profile and diverse breaches affecting everything from the market for cryptocurrencies to the 2018 Winter Olympic Games in Pyeongchang, South Korea. By one count, in January alone, over 7 million successful breaches were recorded.[5]

B. Consequences of breach

It is clear that cyber attacks have very real practical consequences for organizations. Reports of the WannaCry and Petya incidents make for almost apocalyptic reading: "shipping containers could not be loaded, lawyers were locked out of their computers and a production line was prevented from churning out chocolates".[6] Another account begins "[in Britain], doctors could neither access their patients' files nor make appointments to see those patients. In Russia, hundreds of the interior ministry's workers sat idle. In China, students were locked out of their theses".[7]

---

3 Taylor Armerding, *The 17 biggest data breaches of the 21st century*, CSO (Mar. 29, 2018, 12:26 PM), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

4 ICIJ Investigation, *Paradise Papers: Secrete of the global elite*, International Consortium of Investigative Journalistst (Mar. 29, 2018, 12:29 PM), https://www.icij.org/investigations/paradise-papers/.

5 Lewis Morgan, *List of data breaches and cyber attacks in January 2018*, IT Governance (Mar. 29, 2018, 12:31 PM), https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-january-201-2/.

6 Hannah Kuchler, *Cost of cyber crime rises rapidly as attacks increase*, Financial Times (Mar. 29, 2018, 12:31 PM), https://www.ft.com/content/56dae748-af79-11e7-8076-0a4bdda92ca2.

7 The Economist Group Limited, *A large-scale cyber-attack highlights the structural dilemma of the NSA*, The Economist (Mar. 29, 2018, 12:31 PM), https://www.economist.com/news/science-and-technology/21722026-americas-national-security-agency-torn-between-defending-computer-systems-and.

The key concern for most organizations is the financial cost of cyber breaches. At its current rate, the cost of breaches to businesses worldwide is expected to reach $6 trillion by 2021.[8] Such financial consequences for organizations usually manifest themselves by way of regulatory action and/or market response. Take for example the Epsilon breach, which was disclosed to shareholders on 30 March 2011. Here, one of United States' most prominent email service providers succumbed to a spearphishing attack[9] and the email addresses of its clients were obtained by hackers who in-turn subjected these organizations to a sustained spearphishing campaign consisting of an estimated 6 billion spam emails. The estimated cost of the breach to Epsilon emanating from, amongst other factors, reputational damage suffered, when last calculated was projected to top $4 billion.[10] Additionally, Uber are currently under investigation and facing the prospect of hefty fines from the Information Commissioner's Office (ICO) in the UK as well as equivalent regulatory bodies in the United States and Italy for their handling of a data breach in 2016. Instead of reporting a breach, which compromised the personal information of 57 million drivers and customers, the company paid a ransom to hackers and the company proceeded to cover up the incident.[11]

Many professional services organisations are now turning to cyber risk insurance as a means of lessening the inevitable financial damage caused by a potential breach. The Financial Times notes that the London insurance market, the largest in the world, saw a 50% rise in the number of companies and individuals taking out cyber risk insurance policies in 2016. It estimates that the current total written premium amount of $2.5 billion could reach $20 billion by 2025.[12] Due in-part to the ever-increasing quantity and complexity of attacks, cyber risk insurance is typified by high cost and complex coverage terms.[13] Yet, the lack of data about cyber risks poses a problem of coverage for those seeking or currently holding such policies and means that current cyber risk policies are both

---

8 The Editors at Cybersecurity Ventures, *Cybercrime Report*, Cybersecurity Ventures (Mar. 29, 2018, 12:35 PM), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

9 Spearphishing is an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer - *What is Spear Phishing?*, Kaspersky (Mar. 29, 2018, 02:59 PM) https://www.kaspersky.co.uk/resource-center/definitions/spear-phishing.

10 Ross Kerber & Brenton Cordeiro, *Analysis: Alliance Data may face high Epsilon breach costs*, Reuters (Mar. 29, 2018, 12:45 PM), https://www.reuters.com/article/us-alliance-epsilon-costs/analysis-alliance-data-may-face-high-epsilon-breach-costs-idUSTRE7393E320110411.

11 Financial Times Reporters, *Uber faces investigations by regulators over massive data breach*, Financial Times (Mar. 29, 2018, 12:50 PM), https://www.ft.com/content/20d98370-cf68-11e7-9dbb-291a884dd8c6.

12 Madhumita Murgia & Oliver Ralph, *Boom in cyber attack insurance predicted to gather pace,* Financial Times (Mar. 29, 2018, 12:51 PM), https://www.ft.com/content/a767e518-c91e-11e6-8f29-9445cac8966f.

13 Sean B. Cooney, *Untangling the Mystery of Cybersecurity Insurance*, Keesal, Young & Logan (Mar. 29, 2018, 12:31 PM), http://www.kyl.com/2017/02/01/untangling-the-mystery-of-cybersecurity-insurance/ originally appeared in, Law Journal Newsletters (Mar. 29, 2018, 12:54 PM), http://www.lawjournalnewslet-

increasingly expensive and inadequate for many organisations' needs. A report from the SANS Institute highlights the coverage gaps caused by uncertainty in the buying and underwriting relationship between information security personnel (InfoSec personnel) from organisations and insurers. Gaps include: i) technology – InfoSec personnel have a diverse understanding of risk and think in terms of eliminating threats and vulnerabilities by way of policies and programmes, while insurers see risk as the financial loss to a firm from a breach; (ii) assessment – insurers prefer quantitative assessment models, while only 25% InfoSec personnel opt for quantitative models when measuring and benchmarking defences; (iii) communication – gaps in (i) and (ii) have created communication gaps between the InfoSec personnel and the insurer, the InfoSec personnel and risk manager and between the insurer and brokers; and (iv) investment – lack of transparency in underwriting criteria and complex terminology in written policies has resulted in misaligned investment by buyers and the rejection of claims. [14]

C. Human behavior as an aspect oy cyber security

One defining feature of organisational cyber security that has emerged in recent years is that the weakest link in defence infrastructure is humans. When perimeter software defences, such as firewalls, are circumvented, the next – and often last – layer of defence is made up of the employees. This places a premium on their ability to detect and appropriately deal with the attack. Not surprisingly, because the implementation of software protection - when compared with the changing of employee behaviour toward good cyber security - is easier to do, organizations have tended to focus on software protections as a means of defence in the hope of insulating employees from attack. However, software protections carry issues of their own. They are dated by their very nature, and so once rolled out, hackers will set to work developing programmes to hone in on perceived weaknesses. Furthermore, there is evidence of human weakness in the coding of such software protections. A study produced by researchers at the University of Florida, Pennsylvania State University and NYU, puts forward that developers have a heuristics-based decision-making process, which is a computational model of solving problems without considering all the information available. Software vulnerabilities can be explained as elements left out of this mental computational model, or blind spots. [15]

---

ters.com/sites/lawjournalnewsletters/2017/02/01/untangling-the-mystery-of-cybersecurity-insurance/?kw=Untangling%20the%20Mystery%20of%20Cybersecurity%20Insurance&et=editorial&bu=Law%20Journal%20News&cn=20170201&src=EMC-Email&pt=Cybersecurity%20Law%20%26%20Strategy&slreturn=20180229065318.

14 Barbara Filkins, *Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey*, SANS Institute (Mar. 29, 2018, 12:57 PM), https://www.sans.org/reading-room/whitepapers/analyst/bridging-insurance-infosec-gap-2016-cyber-insurance-survey-37062.

15 Justin Cappos, Nicole Morin, Daniela Oliveira, Marissa Rosenthal, Martin K.-C Yeh., & Yanyan Zhuang, *It's the Psychology Stupid: How Heuristics Explain Software Vulnerabilities and How Priming can Illuminate Developer's Blind Spots*, Proceedings of 30th Annual Computer Security Applications Conference, ACSAC (2014).

While software protections are a crucial part of any organization's cyber defence infrastructure, the above vulnerability notwithstanding, they are only a part. A part which is breached from time to time, and once hackers are inside these perimeter defences, unskilled and unaware employees are powerless to stop them. The IBM Security Intelligence Index 2014 noted that 95% of all cyber breaches involve some element of human error.[16] This data was backed up by the Verizon 2016 Data Breach Investigations Report, which also gave examples of how human error manifests itself in a cyber breach.[17] The report notes that basic cyber defences, policies and defence action plans are sorely lacking within organizations; 63% of attacks involve the use of weak, default or stolen passwords; and that a sizeable portion of attacks exploit known vulnerabilities that the target has not patched, despite the patch being available to the user. The report notes that the top 10 known vulnerabilities accounted for 85% of successful breaches. [18]

We have seen that the dominant – and most successful – means of exploiting human weakness in an organization is by way of social engineering attacks (those which involve psychological deception and manipulation) such as spearphishing. As computer security specialist, Bruce Schneier commented back in 2000, "only amateurs attack machines; professionals target people".[19] The Symantec 2017 Internet Security Threat Report notes that in 2016, Business Email Correspondence (BEC) spearphishing emails targeted over 400 organizations per-day and had yielded over $3 billion in stolen information in the years 2013 to 2015.[20] Many of the most prominent data breaches in recent years have relied on this very technique. These include, as mentioned above, the Panama and Paradise Papers hacks of law firms Mossack Fonseca and Appleby respectively. Perhaps one of the best examples of the simplicity of spearphishing and the cataclysmic effect it can have should it be successful, is the Sony hack from late 2015. In the run up to the attack, Sony had been promoting its upcoming feature film 'The Interview', a comedy parodying North Korean leader Kim Jong Un and a plot by American agents to assassinate him. North Korea, infuriated by this apparent show of disrespect, commissioned a hacking group to infiltrate Sony's network in the lead up to the film's release, as confirmed by the FBI.[21] However, the hackers did not attack the organization's perimeter defences, such as firewalls. Instead,

16 *IBM Security Services 2014 Cyber Security Intelligence Index*, IBM Global Technology Services (Mar. 29, 2018, 12:57 PM), https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.

17 *2016 Data Breach Investigations Report*, Verizon (Mar. 29, 2018, 01:00 PM), http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

18 Ibid.

19 Bruce Schneier, *Crypto-Gram*, Schneier on Security (Mar. 29, 2018, 01:02 PM), https://www.schneier.com/crypto-gram/archives/2000/1015.html#1.

20 *Internet Security Threat Report (ISTR) 2018*, Symantec (Mar. 29, 2018, 01:04 PM), https://www.symantec.com/security-center/threat-report.

21 Kara Scannell, *FBI details North Korean attack on Sony*, Financial Times (Mar. 29, 2018, 01:06 PM), https://www.ft.com/content/287beee4-96a2-11e4-a83c-00144feabdc0.

they sent carefully crafted emails to Sony employees purporting to be from Apple, demanding that they confirm their Apple ID credentials as they had detected unauthorised activity. Unwitting employees who clicked on the link in the email were then taken to a page resembling account verification pages used by Apple, where they proceeded to enter their credentials – data which was collected by the hacking group, who then used these stolen credentials to enter the network and upload malware, crippling the system.[22] As Stuart McClure, former CTO of McAfee, notes, many of those who had their data corrupted and then hard-wired in to the malware that was created had significant access to the Sony network.[23] The fallout of the breach has been well documented. Hackers obtained: every employee email for the previous 10-year period, including embarrassing email traffic between executives and Hollywood stars that were subsequently published online; the salaries and personnel records of thousands of Hollywood stars; and several unreleased feature films. It also laterally affected other organizations. For example, secret acquisitions by the social media organization Snap were made public, having been detailed in the leaked emails.[24] The Interview was subsequently pulled by Sony and never made it to the big screen.

In addition to the propensity of unaware employees to fall for a spearphishing attack, decision making within the organization concerning critical elements of security infrastructure demonstrates a glaring lack of awareness of, and appreciation for the risk. Decisions are often based on heuristics, or incomplete mental models similar to the programmer blind spot referred to above, which try to take a reductionist approach to cyber security investment and strategy decisions.[25] One example is the ransom payment and cover-up operation attempted by Uber in the wake of a breach suffered in 2016. Failings in security infrastructure decision making played a key role in a high-profile breach in 2017 involving the National Health Service in the UK, which fell afoul of the WannaCry attack. The WannaCry attack was a worldwide self-propagating cyber attack (having the ability to spread and cause widespread infection without any user interaction) that exploited a vulnerability in Microsoft Windows operating system using a hacking tool called EternalBlue. While Microsoft had, months in advance, release a patch and notification to warn users to repair the vulnerability[26], a number of organizations did not heed the warning, and it was these organizations – from FedEx to various state governments of India -

---

22 Gregg Keizer, *Sony hackers targeted employees with fake Apple ID emails*, Computerworld (Mar. 29, 2018, 01:07 PM), https://www.computerworld.com/article/2913805/cybercrime-hacking/sony-hackers-targeted-employees-with-fake-apple-id-emails.html.

23 Ibid.

24 Alex Altman & Alex Fitzpatrick, *Everything We Know About Sony, The Interview and North Korea*, Time (Mar. 29, 2018, 01:08 PM), http://time.com/3639275/the-interview-sony-hack-north-korea/.

25 Vaibhav Garg & Jean Camp, *Heuristics and biases: implications for security design*, 32, IEEE TECHNOLOGY AND SOCIETY MAGAZINE, 73–79 (2013); see also: Heather Rosoff, Jinshu Cui & Richard S. John, *Heuristics and biases in cyber security dilemmas*, 33, ENVIRONMENT SYSTEMS AND DECISIONS, 4 (2013).

26 *MS17-010: Security update for Windows SMB Server: March 14, 2017*, Microsoft (Mar. 29, 2018, 01:10 PM), https://support.microsoft.com/en-us/help/4013389/title.

that were inevitably affected. For the UK National Health Service, which is publicly funded and chronically over-stretched in terms of resources, warnings about the vulnerability caused by running Windows XP operating system – perhaps the most likely operating system to succumb to an attack that exploited basic weaknesses such as the WannaCry attack – were received even before Microsoft issued the patch notification.[27] Once the WannaCry attack spread to the UK National Health Service, more than 70,000 devices including computers, MRI machines, blood-storage refrigerators and theatre equipment was affected and hospitals and trusts across the UK were forced to turn away non-critical patients.[28] To be sure, this was not a software issue. This was a prime example of the impact of human error on the cyber defence posture of an organization.

D. Legal services

Behind every headline-grabbing IPO, market-shaping antitrust dispute, sub-Saharan hydro-electric dam project, and even the commercial aircraft traversing the skies, there are law firms undertaking mission-critical work to ensure such projects secure financing, comply with regulatory requirements and helping their clients deliver on time and within budget. Owing to law firms' heavy involvement in such matters, and the client rosters that firms boast, they inevitably play host to vast troves of crucial commercially sensitive information. Law firms also serve to filter out information that is not relevant to a particular transaction or dispute, in effect honing the information they hold down to only the most important. It is little wonder then that law firms have become a prime target for hackers in recent years. In 2011, the FBI briefed 200 of the largest US law firms, warning them that hackers see attorneys as the back door to valuable client data, and stressed that such firms were beginning to experience an uptick in spearphishing attacks.[29] This prediction turned out to be startlingly accurate. The opening paragraph of the ABA Tech Report on Security 2015 reads: "law firm data breaches are continuing. It was recently reported that at least 80% of the largest 100 law firms, by revenue, have been hacked since 2011"[30]. The trend has been mirrored in the UK, with a new report from the National Cyber Security Centre noting that 65% of all UK legal services firms have been hacked. [31]

---

27 Mark Evans, Leandros A. Maglaras , Senior Member, IEEE, Ying He & Helge Janicke, *Human behaviour as an aspect of cybersecurity assurance*, 9, SECURITY AND COMMUNICATION NETWORKS, 17 (2016).

28 Amyas Morse, *Investigation: WannaCry cyber attack and the NHS*, National Audit Office (Mar. 29, 2018, 01:13 PM), https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

29 Ivan Hemmans & David G. Ries, *Cybersecurity: Ethically Protecting Your Confidential Data in a Breach-A-Day World*, American Bar Association (Mar. 29, 2018, 01:14 PM), https://www.americanbar.org/content/dam/aba/multimedia/cle/materials/2016/04/ce1604lpi.authcheckdam.pdf.

30 David Ries, *Security*, American Bar Association Techreport 2015 (Mar. 29, 2018, 01:17 PM), https://www.americanbar.org/content/dam/aba/publications/techreport/2015/security/Security.authcheckdam.pdf.

31 *Cyber threats to the legal sector and implications to UK businesses*, National Cyber Security Centre (Mar. 29, 2018, 01:19 PM), https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Cyber-threats-to-the-legal-sector-and-implications-to-UK-businesses.pdf.

While the majority of law firm data breaches go unreported – for reasons we will consider later – some breaches have played out on a very public stage. In early 2016, unsealed criminal charges revealed that a small group of Chinese hackers pinpointed 48 prominent UK and US law firms with expertise in M&A work for the majority of the Fortune500, including Cravath, Swaine & Moore LLP and Weil Gotshal & Manges LLP, and subjected them to a sustained spearphishing campaign over 3 consecutive months.[32] At least one employee at two of the organizations targeted inadvertently granted the hackers access by clicking on a malware-loaded link in an spearphishing email. Once inside the firms' systems, the hackers proceeded to peruse client files and communications relating to at least 10 ongoing or potential deals. The Financial Times notes that in one particularly successful instance, the hackers obtained information relating to Pitney Bowes' offer for Borderfree and Intel's acquisition of Altera and were able to trade ahead of the deals reaching fruition, generating approximately $4 million in the process. [33]

April 2016 also saw the announcement of what has since been dubbed "the biggest leak in data journalism history", the Panama Papers.[34] Here, an internationally operating law firm, Mossack Fonseca, was running two websites. One front facing and one acting as a client interface, the latter of which shared its IP address with the firm's email server, which itself was running a version of Microsoft Outlook not updated since 2009. This effectively meant that obtaining access to the firm's already extremely vulnerable email server would accelerate access to the firm's customer interface, thereby unlocking confidential client information. When this vulnerability was inevitably exploited, 11.5 million documents containing 2.6 terabytes of data were exposed, principally detailing the tax affairs of high profile figures across the world from Russian oligarchs to the Icelandic prime minister.[35] A similar, but unrelated, incident occurred later in 2016, and which was publicly disclosed in October 2017, when major offshore firm Appleby, was breached in an "illegal computer breach"[36], believed to have been carried out using similar techniques to those deployed in the Panama Papers breach. In this instance, 13.4 million documents compris-

32 *United Strates of America vs. Iat Hong, Bo Zheng & Chin Hung*, United States District Court Southern District of New York (Mar. 29, 2018, 01:23 PM), https://www.justice.gov/usao-sdny/press-release/file/921006/download.

33 Brooke Masters, *Lawyers and accountants are prime targets for cyber attacks*, Financial Times (Mar. 29, 2018, 01:26 PM), https://www.ft.com/content/f52f6fee-ccf4-11e6-864f-20dcb35cede2.

34 Barb Darrow, *How Tech Made the Pulitzer Prize-Winning Panama Papers Coverage Possible*, Fortune (Mar. 29, 2018, 01:27 PM), http://fortune.com/2017/05/30/panama-papers-data-tools/.

35 *Offshore Leaks Database*, The International Consortium of Investigative Journalists (Mar. 29, 2018, 01:07 PM), https://offshoreleaks.icij.org/.

36 John Hyde, *Paradise Papers firm Appleby: We've done nothing wrong*, The Law Society Gazette(Mar. 29, 2018, 01:30 PM), https://www.lawgazette.co.uk/practice/paradise-papers-firm-appleby-weve-done-nothing-wrong/5063566.article.

ing 1.4 terabytes of data were obtained and published, exposing the tax workings of companies such as Nike and Apple, as well as high profile figures such as F1's Lewis Hamilton and the Queen of England. [37]

"Consider litigators unable to access motions on a deadline. Trial lawyers preparing for arguments without key documents. Transactional lawyers unable to communicate with clients attempting to close multibillion-dollar deals".[38] This was reality for global heavyweight DLA Piper in June 2017 when the firm fell victim to the Petya attack, another aggressively self-propagating attack similar to the earlier WannaCry attack, which also exploited vulnerabilities in Microsoft operating systems. Interestingly, experts noted that the malware used in the attack was not designed to make money, but instead to spread fast and cause damage.[39] While DLA Piper may not have been held to ransom, the damage caused to the firm by way of disruption of its global operations nevertheless caused significant financial damage. With an estimated 24 hours without phones, 2 days with no access to email and up to 6 weeks without full access to previous emails and other documents, not to mention the lasting reputational damage that comes with such a high-profile breach, it is not surprising that this 'disaster' is likely to end up costing the firm millions in lost earnings.[40]

Cyber attacks are not reserved for only large law firms. Information presented in the ABA Tech Report 2016 demonstrates that while 26% of firms with 500 or more attorneys, and 20% of firms with 100 or more reported successful data breaches in 2015, 25% of firms with between 10 and 49 attorneys and 8% of solo practitioners reported successful breaches over the same period.[41] When one considers that of the 1,300,705 practicing attorneys in 2015, 45% were solo practitioners and only 16% comprised of firms with 100 or more attorneys, it becomes clear that private practice entities of all sizes are under attack.[42] For

---

37 *The Long Twilight Struggle Against offshore Secrecy*, The International Consortium of Investigative Journalists (Mar. 29, 2018, 01:32 PM), https://www.icij.org/investigations/paradise-papers/.

38 Roy Storm, *Ransomware Attack on DLA Piper Puts Law Firms, Clients on Red Alert*, The American Lawyer (Mar. 29, 2018, 01:33 PM), https://www.law.com/americanlawyer/almID/1202791614770/Ransomware-Attack-on-DLA-Piper-Puts-Law-Firms-Clients-on-Red-Alert/.

39 Iain Thomson, *Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide*, The Register (Mar. 29, 2018, 01:35 PM), https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/.

40 https://blog.barkly.com/dla-piper-petya-ransomware-attack; See also: Barney Thompson, *DLA Piper still struggling with Petya cyber attack*, Financial Times (Mar. 29, 2018, 01:38 PM), https://www.ft.com/content/1b5f863a-624c-11e7-91a7-502f7ee26895.

41 David Ries, *Security*, American Bar Association Techreport 2016 (Mar. 29, 2018, 01:41 PM), https://www.americanbar.org/content/dam/aba/publications/techreport/2016/security/security.authcheckdam.pdf.

42 *ABA National Lawyer Population Survey*, American Bar Association (Mar. 29, 2018, 01:45 PM), https://www.americanbar.org/content/dam/aba/administrative/market_research/Total%20National%20Lawyer%20Population%201878-2017.authcheckdam.pdf.

example, in addition to major law firm data breaches referred to above, QBE, a UK insurance company, in a piece with the Financial Times disclosed 150 incidences of successful 'Friday fraud' whereby hackers had learned that UK property lawyers tended to close deals on Fridays and move money between accounts. Hackers proceeded to gain access to firms' email servers via spearphishing campaigns, and once inside, send emails from the server pretending to be the lawyer on the file for that particular transaction and direct closing monies to be transferred to a particular bank account. The claims manager of QBE is quoted as saying "anyone with half a brain could carry out these sorts of email scam ... high street conveyancing firms are not necessarily going to have the latest data security systems". The company estimates that upward of £85 million was stolen over an 18-month period from 2015. This also serves to highlight that there is now a broader spectrum of perpetrators of attacks which range from government-funded hacking groups, such as the Chinese group behind the Canadian Seven Sisters law firm breach in 2010[43], to non-tech-savvy individuals who can buy and distribute malware that even comes with a money-back guarantee should the programme be caught by antivirus systems.

II. PART 2 – THE LAW FIRM CYBER SECURITY QUAGMIRE

While all industries that handle valuable data are subject to increasing levels of cyber attack, there is a set of inter-related factors in the law firm cyber security ecosystem that makes law firms more susceptible to attack and also serves to prevent such firms from taking action to counteract attack vulnerability. As a result of the inter-related external and internal factors affecting law firm cyber security, the human element of firm security infrastructure has been neglected, thereby making humans, at once law firms' greatest asset, their main cyber security weakness.[44] There has been some movement of late, and regulators and clients alike are right to demand law firms do more to improve their cyber security posture.[45] However, much of the scrutiny to which their conduct has been subjected has tended to overlook the complexities of the law firm cyber security quagmire, and unless these issues are addressed in the context of a potential solution, meaningful change is not likely. What follows is an analysis of current issues concerning law firm cyber security and how these, together, create human vulnerabilities ranging from increased susceptibility to spearphishing attempts to a complete lack of awareness of good cyber practice generally, that have the potential, when exploited, to cripple a firm's IT infrastruc-

43 Jeff Gray, *Hackers linked to China sought Potash deal details: consultant*, The Globe and Mail (Mar. 29, 2018, 01:37 PM), https://www.theglobeandmail.com/technology/tech-news/hackers-linked-to-china-sought-potash-deal-details-consultant/article534297/.

44 Russell G. Pearce & Eli Wald, *The Relational Infrastructure of Law Firm Culture and Regulation: The Exaggerated Death of Big Law*, 42, HOFSTRA LAW REVIEW 109 (2013).

45 Julie Sabowale, *Law firms must manage cybersecurity risks*, American Bar Association Journal (Mar. 29, 2018, 01:47 PM), http://www.abajournal.com/magazine/article/managing_cybersecurity_risk; See also: McNerney, Michael & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, AMERICAN UNIVERSITY LAW REVIEW 62, 1243-1272 (2013).

ture, jeopardize client information, and negatively affect reputational capital in the process.

A. The buyer's market for legal services

Commentators such as Ribstein[46] and Galanter and Henderson[47] make the point that the information asymmetry that once existed between law firm and client and was the "bread and butter"[48] of large law firms' reputational capital, which enabled firms to demand high fees, has now been eroded. This is due to in-house legal teams becoming larger and more sophisticated, and because of the variety of service providers on offer in the market, from other law firms to legal technology companies. Clients now have less need to purchase legal services based on personal relationships or sole-provider agreements with traditional firms and are empowered to shop around for the best fit for their particular needs.[49] It is true to say that we now find ourselves in a buyer's market for legal services, where clients' have more control than ever when it comes to who is providing the service and on what terms. Law firms face unprecedented competition from competitor firms, new technologically-enabled entrants and alternative business model (ABS) providers.[50] This shift towards a buyer's market for services was accelerated by the Great Recession and has since seen in-house teams commanding greater bargaining power while operating within tighter budgetary constraints and demonstrating an increased willingness to unbundle work and source it to the most cost-efficient provider. The knock-on effect for traditional law firms is that they have been forced to adapt quickly, or face forfeiting market share. In order to do so, as well as being more receptive to fixed and alternative fee arrangements, law firms have enthusiastically championed a culture of round-the-clock availability to clients, made possible by remote mobile devices[51], and have begun to engage legal process outsourcing and artificial intelligence tools as part of an efficiency and innovation drive.[52]

While law firms have benefitted greatly from modern technological developments, a disparity exists between the hyper rate at which law firms are adopting new technologies and the level of competence of their security infrastructure, which greatly increases the risk of cyber attacks. One example is with regard to smartphones. The ABA Tech Report 2016

---

46 Larry E. Ribstein, *The Death of Big Law*, WISCONSIN LAW REVIEW, 749 (2010).

.47 Henderson William D. & Galanter Marc, *The Elastic Tournament: The Second Transformation of the Big Law Firm*, MAURER SCHOOL OF LAW: INDIANA UNIVERSITY (2008).

48 Russell G. Pearce & Eli Wald, *The Relational Infrastructure of Law Firm Culture and Regulation: The Exaggerated Death of Big Law*, 42, HOFSTRA LAW REVIEW 109 (2013).

49 Ibid.

50 *The Future Of Legal Services*, The Law Society (Mar. 29, 2018, 01:48 PM), https://www.lawsociety.org.uk/news/documents/future-of-legal-services-pdf/.

51 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

52 Ibid; See also McNerney, Michael & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, AMERICAN UNIVERSITY LAW REVIEW 62, 1243-1272 (2013).

notes that 93% of lawyers use a smartphone for work outside of the office, and only 43% of lawyers reported having a mobile technology policy for their firm, meaning that most firms do not have a policy for how mobile devices should be used or client data transmitted or stored on them.[53] As McNerney and Papadopoulos point out, "client relations require near-constant accessibility to attorneys and online access to important documents that might otherwise stay secured in the office".[54] While adequate for meeting modern client availability demands in this way, remote connected devices without robust security measures also "means easier access to sensitive information for adversaries and creates opportunities for hackers to enter onto corporate networks by breaking into remote systems or compromising mobile devices".[55]

B. Lack of regulatory scrutiny and effective ethics rules

In the United States, most state-level legislation requires law firms to notify clients if they reasonably believe a third party has gained unauthorized access to their data, and federal laws apply to particular industries, imposing data security requirements which may apply to lawyers operating within that industry.[56] 47 states have enacted data breach notification statutes which require private entities to notify affected individuals of data breaches compromising their information. The regulations, however, vary wildly as regards which entities must comply, the definition of breach, the definition of reasonable and notification requirements. In the absence of an established federal-level standard of law firm cyber regulation, states have promulgated their own rules. However, few legal standards apply to law firm data breaches, and those that do, such as an obligation to notify clients if one reasonably believes there has been a data breach compromising client information, come with little by way of guidance. This precipitates imprecise and inconsistent interpretation, thereby stifling enforcement.[57] In the UK, the situation is somewhat more straightforward in terms of the regulatory framework, but similar issues persist, particularly regarding notification requirements. Under the Data Protection Act 1998, which is enforced by the Information Commissioner's Office (ICO), the Seventh Principle stipulates that 'appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data,' mandating the implementation of some form of cyber defence by law firms. While in the United States there is a basic requirement in most states to notify

53 Aaron Street, *Mobile Technology*, American Bar Association Techreport 2016 (Mar. 29, 2018, 01:49 PM), https://www.americanbar.org/groups/law_practice/publications/techreport/2016/mobile.html.

54 McNerney, Michael & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, AMERICAN UNIVERSITY LAW REVIEW 62, 1243-1272 (2013).

55 Ibid.

56 McNerney, Michael & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, AMERICAN UNIVERSITY LAW REVIEW 62, 1243-1272 (2013).

57 Madelyn Tarr, *Law Firm Cybersecurity: The State of Preventative and Remedial Regulation Governing Data Breaches in the Legal Profession*, 15, DUKE LAW & TECHNOLOGY REVIEW 234-252 (2017).

affected clients of data breaches (which is seldom enforced for reasons explained above), there is no legal obligation to report breaches which result in loss, release or corruption of client data under the UK regime.[58]

Wald highlights the consequences that a lax regulatory environment for law firm cyber security conduct has had for the ability for market controls – such as action by clients (e.g. firing and/or suing their legal service provider) – to have an impact. Law firms are under no general duty to report attacks or breaches to clients and often have insufficient information about such attacks or breaches to allow for comprehensive reporting to clients in any event. He notes that "a plaintiff in a malpractice lawsuit must establish four elements: the existence of a duty, breach of the duty owed, causation, and damages. Yet a plaintiff in a malpractice suit alleging negligence in failing to protect information is unlikely to be able to prove damages because of the challenges in answering key questions about cyber security breaches: who perpetrated the cyber attack; what information did they steal; what is the value of that information to them or others; and what other harms, such as operational disruption, competition, or reputational damage, resulted for the victim? Consequently, there are hardly any cases litigating attorney (or even corporate) negligence for failure to protect confidential information".[59] That is, of course, if the client is even told about the breach in the first place. Wald refers to this issue as the 'underregulation' of law firm cyber security conduct, or "the inability of clients to effectively utilize liability rules and market controls to ensure that lawyers face appropriate cyber incentives."[60] He goes on to emphasise that "as lawyers face insufficient incentives to implement appropriate cyber security measures and report attacks to clients, data about attacks and their consequences goes uncollected, diminishing the prospect of effective liability rules and market controls developing in the future. This is the kind of market failure that is unlikely to resolve itself without regulatory intervention, except that liability rules are not likely to constitute an effective regulatory response. It is also the kind of market failure that prevents the collection of the very data we need to better understand the extent of the problem we are facing."[61]

Ethics rules, while having a potentially important role to play in improving law firm cyber security conduct should they be upgraded to account for failings in the current regulatory landscape, do little to improve the situation at present. The ABA Model Rules of Professional Conduct have been revised in recent years to take account of the permeation of technology throughout the practice of law and to acknowledge the increased risk of cyber

---

58 *Notification of data security breaches to the Information Commissioner's Office (ICO)*, International Commissioner's Office (Mar. 29, 2018, 01:53 PM), https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf.

59 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

60 Ibid.

61 Ibid.

attacks on law firms. In particular, new Rule 1.6(c) states that "[a] lawyer shall make reasonable efforts to prevent . . . the unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," and is accompanied by Comments 18 and 19 for guidance on interpretation. However, Wald makes the point that efforts to enable ethics rules to fill the void left by fragmented state and federal law firm cyber security regulations fall short of the mark.[62] The Rule and Comments fail to require law firms to put in place a cyber security plan to monitor cyber defences for breach, do not provide guidance on what constitutes "reasonable efforts" and "reasonable precautions", and stop short of mandating disclosure requirements to clients regarding breaches which concern client data.[63] In the UK, lawyers are under an obligation contained in the Solicitor's Regulatory Authority's Code of Conduct 2011 to protect client confidentiality. In particular, Outcome (4.5) stipulates that law firms have effective systems and controls in place to enable them to adequately identify risks to client confidentiality and to mitigate those risks, and Indicative Behaviour (4.1) requires that "your systems and controls for identifying risks to client confidentiality are appropriate to the size and complexity of the firm or in-house practice and the nature of the work undertaken, and enable you to assess all the relevant circumstances". Yet interestingly a recent CenturyLink white paper concerning law firm cyber security in the UK puts forward that only 1% of all complaints received by the SRA are in relation to data security.[64] This serves to reinforce Wald's point that the uncertainty surrounding cyber attacks on law firms – who perpetrated the attack, what information was compromised, and what damage, if any, did clients suffer as a result of the attack - which persists because of uncollected data owing to underregulation, renders liability and market controls ineffective means of regulating lawyers' cyber security conduct.[65]

C Changes in the regulatory environment and client demands

The introduction of the General Data Protection Regulation (GDPR) in May 2018 introduces far more stringent regulatory standards and obligations on firms to protect data. The GDPR will apply not only to organizations within the EU, but also organizations located outside the EU if they offer services to EU data subjects. With over 100 US law firms located in London alone, the majority of which have European entities on their respective client lists, it is clear that the GDPR is an initiative with global reach. Obligations under the GDPR include mandatory breach notification reporting to the relevant national regulatory body (e.g. the UK ICO) within 72 hours and 'privacy by design' which

62 Ibid.

63 Ibid.

64 *Law firms and cybersecurity: how can lawyers keep their client data confidential?*, CenturyLink (Mar. 29, 2018, 01:51 PM), http://www.centurylink.co.uk/asset/business/enterprise/white-paper/centurylink-law-firms-and-cybersecurity-wp170692.pdf.

65 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

involves implementing appropriate security measures with regard to systems and personnel, and introducing policies and procedures governing data management by staff.[66] Much has been made of the penalties which can be levied against organizations found to breach provisions of the GDPR. A non-compliant firm could face a fine of €20 million or 4% of turnover, whichever is greater. This is doubtless a positive development, and it will be interesting to observe the impact it has on law firm cyber conduct. In-light of the above issues concerning the collection of data on law firm cyber incidents and the issues faced by law firms in identifying breaches in the first place, there is reason to be sceptical. The concern is that law firms will adopt the bare minimum standard of compliance within the realms of their perceived regulatory threat level, which is arguably lower than average organization given the enigmatic nature of law firm cyber security data. However, Article 24 of the GDPR, which concerns the implementation of appropriate technical and organizational measures to protect information, also requires affected organizations to demonstrate compliance with the GDPR. With a recent report highlighting that approximately 25% of UK based law firms believing themselves to be compliant with the provisions of the GDPR, it is true to say that law firms, at a minimum, will be subjected to increased regulatory scrutiny under the GDPR, the above scepticism notwithstanding. It may well be the case that national regulatory bodies turn to use the GDPR in an attempt to force better law firm cyber security – time will tell.

With respect to ethics rules, Wald has made clear that the recent revision of the ABA Rules of Professional Conduct – particularly Rule 1.6(c) and accompanying Comments 18 and 19 stop short of being an effective means of mandating better cyber security in the fact of inadequate liability rules and market pressure. He advocates for a further revision of the Rules to require stronger cyber protections within law firms, provide for mandatory breach disclosure requirements to clients, and delineation on the meaning of 'reasonable' in the context of cyber protections and disclosure requirements upon breach.[67] While it is agreed that the "promulgation of robust rules of professional conduct" concerning security protection in law firms and data breach reporting to clients would in theory incentivise law firms to take action, such radical overhaul – which would need to be an internationally co-ordinated effort on behalf of national regulatory authorities in order to affect globally operating law firms – is not immediately on the horizon.[68]

In addition to the - albeit piecemeal - movements taking place with regard to the regulatory environment and ethics rules concerning law firm cyber security, clients too are beginning to exert market pressure on their legal service providers. The ABA Tech Report on security 2016 suggests that increased pressure from clients – who are themselves examining their cyber security posture and that of their supply chain – is causing firms to focus on cyber risk. 62.8% of law firms with 500 or more and 30.7% of all law firms reporting

66 The EU General Data Protection Regulation (GDPR) (Mar. 29, 2018, 01:50 PM), https://www.eugdpr.org/.

67 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

68 Ibid.

that actual or prospective clients had provided them with security requirements.[69] We know little about the actual figures, however. Some initial research in to law firms in the United States suggests that 40% of firms intend to increase their cyber security spend somewhat in 2018[70], but aside from this, data remains opaque. Liability rules may also inform law firm cyber conduct, notwithstanding the potential issues with compliance highlighted above. Firms which stand accused of poor cyber conduct may simply settle with the affected client instead of having the issue played out in public, which could stand to harm both organizations[71]. Such settlement serves as a form of damage limitation, whereby the firm may pay compensation to an affected client and, in the worst case, lose that client's business, but crucially, information about the breach is kept private in order to protect the firm's reputation.

A potentially important development came by way of a class action suit brought in the District Court for the Northern District of Illinois in April 2016, when a client sued its law firm, not for damage resulting from breach, but because their technology systems were not up to "industry standards", leaving open the possibility that client data could be jeopardised should the firm's systems be breached.[72] While the dispute was eventually arbitrated, meaning that all further information remained private, the initial complaint was unsealed by the court in December 2016. This is interesting for a number of reasons. Firstly, it demonstrates a willingness on behalf of a client to take a proactive approach to enforcement of malpractice liability further upstream than what is usually associated with a malpractice suit. Second, it highlights the effectiveness of the use of alternative dispute resolution provisions in retainers as a means of keeping malpractice issues relating to client information out of public view, meaning that it is likely that data regarding law firm cyber security breaches and disputes will continue to go uncollected. The likely consequence is that there will persist little by way of judicial exposition of aspects of malpractice suits emanating from law firm cyber security conduct, such as what is 'reasonable' in the context of firm's cyber security protections or data breach disclosure requirements to clients, even if we do see an uptick in malpractice actions.

Recent cyber security incidents involving law firms such as the DLA Piper hack and the

---

69 David Ries, *Security*, American Bar Association Techreport 2016 (Mar. 29, 2018, 01:52 PM), https://www.americanbar.org/content/dam/aba/publications/techreport/2016/security/security.authcheckdam.pdf.

70 Robert Half, *Survey: Four In 10 Lawyers Plan To Boost Cybersecurity Spending In Next 12 Months; Budgets To Increase 13 Percent On Average*, Robert Half Legal (Mar. 29, 2018, 01:55 PM), http://rh-us.mediaroom.com/2017-10-19-Survey-Four-In-10-Lawyers-Plan-To-Boost-Cybersecurity-Spending-In-Next-12-Months-Budgets-To-Increase-13-Percent-On-Average.

71 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

72 Sedgwick LLP, *United States: Professional Services Firms Beware: Just Because You Haven't Suffered A Data Breach Doesn't Mean You Won't Be Sued – And the Worst Part, There May Not Be Coverage*, Mondaq (Mar. 29, 2018, 12:41 PM), http://www.mondaq.com/unitedstates/x/575630/Insurance/Professional+Services+Firms+Beware+Just+Because+You+Havent.

Panama and Paradise Papers, which implicated Mossack Fonseca and Appleby respectively, have highlighted what we already know about attacks on law firms, according to Wald. We know law firms are aggressively being targeted, we know more about the type of hackers and why they are attacking law firms. Firms even know more about how to protect themselves from such attacks and how to mitigate damage caused. Importantly, however, we are still none the wiser as to whether law firms are actually acting on this data to improve cyber defences and thereby protect client information.[73]

D The law firm partnership model, PEP success and reliance on the billable hour

As with the original Cravath model, large law firm success continues to be underpinned by time-based billing and billable hour budgets today. The billable hour has itself raised a range of issues since its inception, from the impact that billable hour culture has on lawyers' health, morale and work-life balance to the proposition that it actually tends to reward inefficiency and other unethical practices.[74] As Parker and Ruschena note, the junior lawyers of today in large law firms are under the strong and consistent impression that the value of their work is judged based on the fees they generate in the form of billing and when faced with an employer whose goal is revenue generation for the partners, non-partner lawyers may feel a disconnect in-terms of loyalty to the firm, precipitating issues such as unethical behaviour in relation billing practices and de-motivation regarding firm initiatives.[75] The core decision making of the firm is controlled by the inner-circle of equity partners, who also control access to key clients. Molot notes that because an equity partner's stake vanishes upon retirement, his/her only real reward for partnership is the annual draw on profits during productive years at the firm, meaning they are ill-equipped to make long-term investment decisions in the firm and have a decidedly short-term bias.[76] Law firm partnerships can therefore be said to be short-termist by nature and because firms are obsessed with current comparative performance metrics such as the 'profit-per-equity-partner' (PEP) marker of success, by which firms are ranked against competitors, there is a clear and definite focus on maximizing profits.[77]

This also serves to reinforce a point alluded to earlier with respect to the changing nature of the profession toward a buyer's market for services: that there now exists a culture of 24/7 availability to clients, enabled by remote devices. Lawyers are effectively always connected to the network, and by consequence there is optimal opportunity to generate more fees by way of billing. Molot argues that this development has served to alienate lawyers

---

73 Ibid.

74 Christine Parker & David Ruschena, *The Pressures of Billable Hours: Lessons From a Survey of Billing Practices Inside Law Firms*, 9, UNIVERSITY OF ST. THOMAS LAW JOURNAL 619 (2011).

75 Ibid.

76 Jonathan T. Molot, *What's Wrong with Law Firms? A Corporate Finance Solution to Law Firm Short-Termism*, 88, SOUTHERN CALIFORNIA LAW REVIEW 1 (2015)

77 Ibid.

and clients alike. The, now 24/7, billable hour model serves to maximize current profits, thereby boosting a firm's PEP standing, but leaves clients feeling deeply dissatisfied. Firms' have the wrong financial incentives to do the work and clients also feel overcharged due to inherent inefficiencies of their work practices, while lawyers themselves feel overworked and undervalued.[78]

'Autonomous self-interest' – seeking to maximize one's own atomistic good without regard for others - has replaced 'relational self-interest' – prioritising the inter-relatedness of actors and that maximization of self-interest cannot occur in isolation - as the dominant culture of the legal profession. This has served to undermine both the economic and professional conduct of firms.[79] Galanter and Henderson highlight a further impact of this new model, which is particularly relevant for our purposes: "notwithstanding its formidable size, the 'firm' itself has remarkably little autonomy to pursue noneconomic objectives, such as ... the training and mentoring of the next generation of lawyers. Although the partnership shares the benefits of successful recruitment, the lack of credible risk sharing reduces the willingness of individual lawyers to invest in firm-wide initiatives that do not simultaneously optimize their own practice".[80]

We would add that in an autonomous self-interest culture where partners often strive to 'own' their client relationships and 'eat what they kill' in terms of maximising their own profits based on those 'owned' relationships, there is often a perverse incentive for information hiding and for keeping things from the rest of the partners and the firm. This in turn can lead to riskier and often unethical practices that are often not visible at Firm level. Furthermore, due to law firms' lack of permanent equity, current equity partners, or the decision making core of the firm, have little incentive to invest in projects that are long-term in nature, such as investments in firm IT and infrastructure, as it is likely the benefits of such investment will be seen also in the long term – perhaps after the particular partners charged with making such decisions have retired or moved on to pastures anew. This is despite, as Molot notes, corporate finance literature being replete with evidence that short-termism does not, in fact, serve to maximize returns for equity stakeholders.[81]

E The product of short-termism and underregulation combined

Short-termism, coupled with the underregulation of cyber security conduct, has created a plethora of negative consequences that characterise the current internal law firm cyber security environment. Issues such as the lack of investment in IT and infrastructure projects has severely limited firms' ability to implement adequate cyber security protections,

78 Ibid.

79 Larry E. Ribstein, *The Death of Big Law*, WISCONSIN LAW REVIEW, 749 (2010).

80 Henderson William D. & Galanter Marc, *The Elastic Tournament: The Second Transformation of the Big Law Firm*, MAURER SCHOOL OF LAW: INDIANA UNIVERSITY (2008).

81 Jonathan T. Molot, *What's Wrong with Law Firms? A Corporate Finance Solution to Law Firm Short-Termism*, 88, SOUTHERN CALIFORNIA LAW REVIEW 1 (2015)

while a culture of 24/7 availability to clients enabled by remote connected devices increases vulnerability. In any event, given the absence of effective liability rules and market pressure, law firms are not being forced to change. It is true to say that law firms are taking steps to improve their cyber defences, given the current threat environment. Improving software protections such as firewalls appears to be the obvious first step, but some firms have also moved to tackle the human element of cyber security with awareness campaigns such as 'Cyber Security Month', spearphishing penetration testing (where test spearphishing emails are sent to staff and responses recorded), and corporate training exercises such as tutorials and accompanying exercises. Additionally, some lawyers, as Wald notes, may respond to peer pressure and organically evolving security norms within firms.[82] However, these approaches are inadequate to deal with the persistent and systematic problems caused by law firm short-termism and underregulation generally, but especially the most important aspect of cyber defence - humans. The current approach adopted by law firms means that staff, from administrative staff to partners, are fundamentally under-skilled and unprepared to guard against cyber attacks.

It has been true for some time that cyber security is more a human issue than an IT issue.[83] Improving cyber security conduct therefore necessitates behavioural change on behalf of those within the organization. Such change is a painstaking and slow process, requiring persistent effort and monitoring over time to adjust a current feedback loop to fit the desired behaviour. [84] A short tutorial video, an awareness campaign, or standalone spearphishing penetration testing will not achieve such change. In a recent conversation with the Chief Information Officer of a major UK law firm, the authors learned that the average annual time spent training lawyers within the organization was as little as 8 minutes per year - presumably the length of the mandatory tutorial video and questionnaire, and this was predicted to be the same across the majority of large UK law firms. It has also been well documented that awareness campaigns do not affect behaviour when it comes to cyber security. Analogous data is provided by Evans et al, with respect to the healthcare industry in the UK. The authors note that the National Health Service was successfully breached across its various organizations over 7000 between 2011 and 2014, with an increase in the number of breaches of 101% between 2013 and 2014, all despite 75% of such organizations receiving standard security awareness material over the same period.[85] Finally, spearphishing penetration testing, while perhaps one of the more effective means of monitoring firm cyber security vulnerability to attack, can do little beyond monitoring if not accompanied by regular training in order to affect meaningful behavioural change. This is a development in law firm cyber defence that has been hamstrung by the

---

82 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

83 *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within*, Kaspersky Daily (Mar. 29, 2018, 02:06 PM), https://www.kaspersky.com/blog/the-human-factor-in-it-security/.

84 Shari Lawrence Pfleefger & Deanna D. Caputo, *Leveraging Behavioural Science to Mitigate Cyber Security Risk*, 31, COMPUTERS & SECURITY 4 (2012).

85 Mark Evans, Leandros A. Maglaras , Senior Member, IEEE, Ying He & Helge Janicke, *Human behaviour as an aspect of cybersecurity assurance*, 9, SECURITY AND COMMUNICATION NETWORKS, 17 (2016).

billable hour culture, as firms fail to reconcile effective and regular cyber security training with 24/7 availability to clients.

As we have seen, lawyers unskilled to deal with, and unaware of the dangers of, cyber attacks are the greatest threat to a law firm's security, with many large data breaches in recent years – such as DLA Piper and Appleby – emanating from spearphishing campaigns. The impact of such breaches was exacerbated by the lack of a clear cyber security policy or response plan within the individual firm. In addition to the above issues of short-termism and underregulation being contributing factors to cyber security issues which persist in law firms, an underlying issue that plays a key role in lawyers' susceptibility to attack is their personality type. Research by Halevi, Memen and Nov has demonstrated that conscientious personality types are far more susceptible to spearphishing than other personality types.[86] Conscientiousness is associated with being stable, trustworthy, thorough, analytical and factual – key personality and skills traits of lawyers. The study found that "while conscientiousness people are hardworking and have high self-control ... an appeal to efficiency and order will overcome the participants self-control and raise the likelihood of responding to a spear-phishing attack".[87] The study also showed a negative correlation between respondents' perceived risk of attack versus their actual susceptibility to attack, thereby demonstrating that not only are conscientious types more vulnerable to attacks, they actually underestimate the likelihood of falling victim to an attack.[88] This underlying behavioural weakness is doubtless amplified by the current issues of law firm short-termism and the underregulation of law firm cyber security conduct.

It should be noted that the consequences of inadequate training are not just limited to failing to spot attacks, however. They extend to dangerously ignorant cyber security conduct by personnel online. A recent report released by RepKnight in January, which studied the dark web footprint of the 500 biggest UK law firms, showed that over 1 million leaked, hacked or stolen credentials – including firm email address and password combinations (80% of the credentials) – were available for sale on the dark web. That is an average of 2,000 credentials per firm, and at least 1 from every firm. What is most worrying about this development, notwithstanding the sheer size of the confidential data available, is that most of said data was obtained from third-party breaches, or breaches unconnected to the firm itself. This means that lawyers had been using their work credentials to sign up to these third parties' sites or offerings, apparently completely oblivious to the risk.[89]

---

86 Tzipora Halevi, Nasir Memon & Oded Nov, *Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks*, SSRN (Mar. 29, 2018, 02:14 PM), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544742.

87 Ibid.

88 Ibid.

89 *Securing the Law Firm: Dark Web footprint analysis of 500 UK legal firms*, RepKnight (Mar. 29, 2018, 02:16 PM), https://www.repknight.com/wp-content/uploads/2018/01/White-Paper-Securing-the-Law-Firm-January-2018-Website-LM.pdf.

Lack of investment also means that firms are understaffed in terms of specialist IT personnel to manage cyber risk. Large law firms, especially those spoken to by the authors, operate with small teams of between 4 and 10 cyber risk professionals, severely curtailing their ability to affect cultural change within such large organizations. An interesting consequence of this, which to a large extent is explained by the organizational environment of law firms, is that legal and IT teams operate in silos almost completely disconnected from each other. Legal teams or departments are characterised by autonomous self-interest, prioritising the team instead of the firm as the collective in the pursuit of revenue maximization by way of billing, and the IT team is so small that it is a rare occurrence for the legal team to ever have sight of them, beyond their 8-minute yearly compliance video, of course. At present, IT and cyber security matters are delegated to the IT or IT Risk team, who fix the matter and enable the lawyer to get back to work, with little or no integration or information sharing between the teams. When the IT team attempt to introduce new measures, they are likely to meet resistance on budgetary and personnel fronts. For example, the implementation of new cyber security systems can entail considerable expense and the time spent training-in personnel on such systems (or time not spent billing) would be hard to recover.[90] Additionally, the introduction of security measures such as limiting access to networks or mandating frequent password changes, or the implementation of internal cyber security policies intended to improve conduct within legal teams are likely to be perceived as cumbersome, time-consuming and intrusive for lawyers and therefore are less likely to be followed.[91] Wald refers to these as 'Holmesian bad people', or those who will attempt to get away with not implementing appropriate cyber security measures owing particularly to an acute awareness of the underregulation of law firm cyber security conduct.[92]

III. PART 3 – THE SOLUTION

A The inadequacy of the current approach to training

It should now be clear that law firm cyber security, while in need of drastic improvement, faces significant challenges in order to overcome the inter-related complexities that have curtailed such improvement over time before any real progress can be made. Law firms are moving to shore up cyber defences, but current approaches revolve around software protection, spearphishing penetration testing, inadequate and expensive cyber risk insurance, awareness alliances, sponsored seminars and formal tick-box compliance training for minutes per year. None of these approaches are effective at impacting the human behaviour aspect of cyber security defence, as is clear by the mounting evidence of continued cyber breaches experienced by law firms and lack of appreciation for cyber risk in lawyers'

90 Alex Blau, *The Behavioral Economics of Why Executives Underinvest in Cybersecurity*, Harvard Business Review (Mar. 29, 2018, 02:17 PM), https://hbr.org/2017/06/the-behavioral-economics-of-why-executives-underinvest-in-cybersecurity.

91 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

92 Ibid.

online behaviour, all attributable to human error. These protections represent the best and the most extensive in the legal profession at present.

As outlined earlier, the most effective means of attack is spearphishing. A recent FireEye whitepaper highlights that the most effective means of preventing spearphishing is to first and foremost, "train users to recognise, avoid and report suspicious emails"; second is to "maintain and update security technology and processes to prevent, detect and respond to ever-evolving spear-phishing threats" and thirdly striving "to stay ahead of attackers by investing in actively updated threat intelligence and expertise to meet their needs".[93] The second and third elements of this strategy pose an issue owing to the short-termist nature of law firms, aversion to investment and the difficultly of overhauling systems for globally operating firms. However, the first issue is by some way the most crucial but also the most troublesome for law firms. Effective means of training employees to deal with spearphishing requires persistent testing backed up with context-specific educational training so that employees are regularly educated as to the dangers of spearphishing, know how to detect an attack and what to do when they suspect one, and their susceptibility to attack is constantly tested to promote vigilance and defence skills development[94]. Training is the most important element of defence against spearphishing primarily because it builds skills and awareness to deal with attacks if and when a firm's software defences are penetrated. Additionally, training and awareness are crucial in establishing the foundations of a culture of good cyber practice, with such skills and awareness positively permeating throughout the organization and subsequently impacting the investment decisions of the partnership. A recent report by PhishMe highlights the importance of such training. They note that training employees to spot and report spearphishing emails reduced the average time it took to detect a breach from 146 days to 1.2 hours.[95] In its absence, the partnership is likely to compartmentalise IT and infrastructure spend (including training) as just another budgetary consideration, without the added consideration that such a business risk warrants. Law firms are doubtless aware of the need for such training, and yet it is has almost no prominent role to play within the organization. The reality of short-termism has meant that, for law firms, hourly billing and 24/7 availability to clients and such training are perceived to be mutually exclusive. This consideration also holds true for the other 2 elements of the FireEye whitepaper, with firm-wide IT infrastructure updates likely to be perceived as disruptive and precipitate further lost time. In the face of underregulation of their cyber security conduct, law firms have had little incentive to find a solution to this issue.

---

93 *Best Defense Against Spear Phishing*, FireEye (Mar. 29, 2018, 02:19 PM), https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html.

94 Ibid.

95 *Phishing Defense Guide 2017*, PhishMe (Mar. 29, 2018, 02:20 PM), https://www.ciosummits.com/PhishMe-Phishing-Defense-Guide_2017.pdf.

B Cause for improvement

Arguments abound as to why law firms need to improve cyber security defences. We have noted some key reasons above: attacks are increasing in quantity and complexity; breaches are becoming more common and more high-profile; the impending introduction of the GDPR; clients are demanding a certain standard of cyber protection at the beginning of the relationship; data privacy and data stewardship awareness and perception are becoming much more commonplace; there is a prospect of malpractice suits by aggrieved clients for lax cyber security practices and breach of fiduciary duty to protect information. Furthermore, a successful breach that plays out on the public stage will serve to erode a firm's reputation. For example, in 14 March 2018, Mossack Fonseca – the firm implicated in the Panama Papers – announced that it was to shut down at the end of the month, citing the "reputational deterioration" that occasioned "irreversible damage" on the firm.[96] We would also add that strong cyber defence capability now has key differentiating potential in an ultra-competitive buyer's market for legal services. While law firm cyber security is underregulated, the conduct of their clients, for the most part, is not and carries with it enormous non-compliance costs. For example, organizations in the financial services and healthcare sectors are subject to strict data security laws, which are destined to become more-so upon the introduction of the GDPR this year. Such organizations are under an obligation to require their supply chain to attain a certain level of cyber security protection in order to comply with provisions of the GDPR. If law firms can demonstrate adequate cyber defences when compared to competitors, during the pitch process for example, their chances of being perceived favourably by prospective clients who see cyber security as a critical business risk, are likely to be substantially higher than firms with weaker cyber defences. Firms typically need to show that they have technical expertise, geographical reach, project management protocols and tools to accurately control scope, cost and timing, but now also need to ensure and demonstrate that client information will be subject to the highest standards of information security. Incredibly, should a law firm be in a position to demonstrate the 3 elements of spearphishing protection detailed in the FireEye whitepaper, they would be perceived as market-leading in terms of cyber security protections. As Wald notes 96% of attacks employ simple techniques, such as spearphishing, and yet 97% of attacks can be blocked entirely by the use of common cyber security defence practices that are entirely within reach of law firms today. Such approaches comprise of the technological and human alike: "using current virus scanners and firewalls, installing patches and updates, using cryptographically strong passwords, avoiding risky software downloads from the Internet, eschewing the use of public cloud providers or file sharing services for sharing documents, avoiding the use of web-based e-mail services and public Wi-Fi, replacing the default passwords on network hardware, and training employees to recognize deceptive ("phishing") attacks".[97]

---

96 Reuters Staff, *Panama Papers law firm Mossack Fonseca to shut down after tax scandal*, Reuters (Mar. 29, 2018, 02:21 PM), https://www.reuters.com/article/us-panama-corruption/panama-papers-law-firm-mossack-fonseca-to-shut-down-after-tax-scandal-idUSKCN1GQ34R.

97 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

C. A human problem – insights from behavioral science

The technological protections described by Wald are a must, and to a large extent, already exist in law firms today. The human protections are significantly more important. Given that the vast majority of data breaches (95%) involve some aspect of human error, it is clear that cyber security is a human problem that requires a human solution, with effective training being the most critical component of the passport to success. But how do law firms reach this promised land, given the complex and crippling effects of short-termism and underregulation? To be sure, fundamental tenets of good cyber defence posture will inevitably require investment on behalf of the partnership – in-terms of systems and personnel, and also the implementation and enforcement of stringent cyber security policies, in a coordinated effort by legal and IT teams working together. It is our contention that the most important aspect of law firm cyber defence for our purposes – training employees to deal with spearphishing – which is a crucial defence mechanism in its own right, but also serves to underpin the likely success of such other aspects as policy development and enforcement within legal teams, does not require a dismantling of the short-termism/underregulation conundrum in order to arrive at a workable solution. Instead, what is needed is a change in how such training is perceived and delivered. The current e-learning approach to spearphishing training in law firms (a video tutorial and 'click next' test) is a concept first introduced in the late 1990s[98], and is in dire need of updating. Additionally, we note that some law firms have now made regular spearphishing penetration testing part of their defence protocol. The common approach is to send employees a suspicious email to their work email address and record the response, i.e. whether the recipient clicks on a link contained in the email, marks the email as spam, or ignores the email. One such email that one of the authors received while working for a large UK law firm related to the establishment of a mentoring scheme sponsored by Amazon, whereby Amazon customers who are professionals would sign up to mentor school children and other children from youth organizations in their community. The email immediately raises suspicion. The author concerned did not have an Amazon account set up with the firm's email, and there was therefore no reason for Amazon to send an email to this address, and so the email was duly marked as spam. Later, in a conversation with the Chief Information Officer of the firm (the same conversation where the authors uncovered the 8 minutes per year training figure), we learned that the spearphishing test sent to the majority of employees in the London office tricked 42% in to clicking on the bogus link in the email. Interestingly, spearphishing awareness information was circulated to those respondents that clicked on the link in the initial test, and when the test was repeated 1 week later with a different template, 75% of those respondents again clicked on the link. This serves to reinforce the point that spearphishing penetration testing, while an effective means of gauging vulnerability to spearphishing attack at any given time, is not effective at developing the skills and awareness needed to adequately defend against attack if not supported and reinforced by effective training with an element of duration.

---

98 Holly Faurot, *LMS 101: The Evolution Of Corporate Learning*, Forbes (Mar. 29, 2018, 02:23 PM), https://www.forbes.com/sites/paycom/2017/02/07/learning-management-systems-101-the-evolution-of-corporate-learning/#48b3e8105e25.

Daniel Solove sums up the need for a change in training methodology as follows: "Security is complicated because it essentially requires each employee to act with a high level of awareness and vigilance, a state that is hard to sustain. Over time, corners tend to get cut more, busy people tend to do more careless things, practices tend to become sloppy. That's human nature. Complacency sets in. Being on one's toes isn't an easy state to maintain. These problems are best addressed through training. Merely showing people a PowerPoint or putting them through a program that's the equivalent to an airline safety video is a waste of time. People must be engaged. They must care. And the message must be repeated over and over and over. People aren't robots, after all. They forget quickly ... The fact is, cyber security training is vastly undercapitalized, and the lack of investment in quality cyber education programs is manifest in the sheer volume of breaches that continue to be rooted in human failure ... To be clear, technology is a critical piece of the cyber security puzzle, but just as with a car containing all the latest safety technology, the best defence remains a well-trained driver".[99]

Appeals to employee engagement and incentivising them to care about security are themes rooted in the behavioural science work of Nobel Economics laureate Dr Richard Thaler and before him Daniel Kahneman and Amos Tversky.[100] Dr Thaler's work with Cass Sunstein on 'nudging', improving behaviour by arranging choice architecture without removing an individual's freedom of choice, has important application for cyber security within organizations. Thaler and Sunstein make the point that an organization's policies are predicated on the principle that its people do not intentionally behave irrationally and yet we fail to recognise our own biases, even if we consider ourselves to be completely rational. At work we don't always do the things that might improve our organization's security.[101]

The concept that nudging can improve organizational cyber defence has been adopted by the UK Centre for the Protection of National Infrastructure (CPNI), who have issued guidance to organizations on how to improve security defences, underpinned by the '5Es' framework: educate employees on why threats exist, the form they take and why they are vulnerable; enable employees to demonstrate the cyber defence skills expected of them; shape the environment to make it easier to demonstrate good cyber defence skills; encourage action by providing feedback to employees to encourage good cyber defence behaviour and skills development while highlighting errors and discouraging undesired actions

---

99 Daniel Solove, *Cybersecurity vs. Humans: The Human Problem Requires a Human Answer*, TeachPrivacy (Mar. 29, 2018, 02:23 PM), https://teachprivacy.com/cybersecurity-vs-humans-human-problem-requires-human-answer/.

100 Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis of Decision under Risk*, 47, THE ECOMETRIC SOCIETY 263-292 (1979).

101 Philip Ebert & Wolfgang Freibichler, *Nudge Management: Applying behavioural science to increase knowledge worker productivity*, 6 JOURNAL OF ORGANIZATIONAL DESIGN 4 (2017); See also: RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008).

and behaviours; and evaluate the impact on employee behaviour by tracking progress in skills development as against the time and resources committed to improving defence skills.[102] The guidance also highlights the importance of endorsement from credible sources in the organization's hierarchy such as C-suite executives as crucial to supporting the success of the framework.[103] Pfleeger and Caputo make the point in their survey paper which illustrates that leveraging behavioural science theory in establishing a defence infrastructure by catering for such elements as cognitive dissonance[104], the bystander effect[105] and confirmation bias[106], leads to clear improvements in employee cyber defence skills and awareness as well as an overall improvement in the effectiveness of organizational cyber defence. They note "most efforts to improve cyber security focus primarily on incorporating new technological approaches in products and processes. However, a key element of improvement involves acknowledging the importance of human behaviour when designing, building and using cyber security technology".[107]

D. Heads-up: A new approach to training using aspects of modern technology

The question remains: how can law firms move to a model that allows for effective spearphishing defence skills development and also establish the key foundations of a culture of good cyber security behaviour generally without detracting from lawyers' availability to clients or disrupting their work environment, which would negatively impact billable targets. We contend that modern technological innovations, when applied to current training methodologies to deal with spearphishing, have a key role in developing a realistic solution to the issue of spearphishing training in law firms. This, in-turn, allows

---

102 *Embedding Security Behaviours: using the 5Es*, Centre for the Protection of National Infrastructure (Mar. 29, 2018, 02:25 PM), https://www.cpni.gov.uk/system/files/documents/98/dc/Embedding-Security-Behaviours-Using-5Es.pdf.

103 Ibid.

104 Cognitive dissonance is the feeling of discomfort that comes from holding two conflicting thoughts in the mind at the same time. Cognitive dissonance is central to many forms of persuasion to change beliefs, values, attitudes and behaviours. To get users to change their cyber behaviour, we can first change their attitudes about cyber security. For example, a system could emphasize a user's sense of foolishness concerning the cyber risks he is taking, enabling dissonant tension to be injected suddenly or allowed to build up over time. Then, the system can offer the user ways to relieve the tension by changing his behavior.

105 The bystander effect is a psychological phenomenon in which someone is less likely to intervene in an emergency situation when other people are present and able to help than when he or she is alone. During a cyber event, users may not feel compelled to increase situational awareness or take necessary security measures because they will expect others around them to do so. Thus, systems can be designed with mechanisms to counter this effect, encouraging users to take action when necessary.

106 Once someone takes a position on an issue, she is more likely to notice or give credence to evidence that supports that position than to evidence that discredits it. Users may have initial impressions about how protected (or not) the information infrastructure is that they are using. To overcome their confirmation bias, the system must provide users with an arsenal of evidence to encourage them to change their current beliefs or to mitigate over-confidence.

107 Shari Lawrence Pfleefger & Deanna D. Caputo, *Leveraging Behavioural Science to Mitigate Cyber Security Risk*, 31, COMPUTERS & SECURITY 4 (2012).

for realistic behavioural change over time and the establishment of a key component of effective law firm cyber defence infrastructure without infringing on the constraints imposed by short-termism and underregulation. It is important to note this is not an abstract or theoretical solution suggested by the authors in light of the above analysis. This technology is already being applied to create non-disruptive, behavioural science-based spearphishing training, with real solutions available to organizations on the market today[108]. The approaches adopted by companies such as Cofense, Wombat and Fissure Security purport to upgrade the current standard of spearphishing training, which at present consists of sporadic spearphishing penetration testing, educational tutorials and the circulation of awareness material, which has little impact on employee cyber security behaviour and competence. These organizations propose continuous, non-disruptive training, as well as behavioural analytics to arrive at a scenario where employees can be tested and trained to improve cyber defence and awareness 24/7 and be provided with accurate feedback on their progress, while also maintaining availability to clients 24/7, as such training does not necessitate employees being removed from their normal work environment and is instead integrated with their work routine.

Such training involves a combination of i) spearphishing penetration testing in the form of distributing fictitious quick-action spearphishing emails (short context specific email containing a link or attachment) and using data analytics to track responses, and ii) an overlay on employees' computer screens that runs when the email application such as Outlook is open, and provides subtle but clear indicators of spearphishing (e.g. drawing users' attention to the email address, reminding users to consider whether any links in the email re-direct to an external website, and whether any attachments are referred to or described in the email or that the email and its attachments were expected by the user). These indicators or pockets of information, such as 'Security Tips', are displayed on screen but in a non-disruptive manner (e.g. small info boxes or coloured indicators in the margins of emails) and also do not require interaction in the form of 'click-to-agree' in order to avoid click fatigue. This training is then continually reinforced with regular spearphishing training emails (similar to the spearphishing penetration testing referred to above) which would target a particular aspect of spearphishing to test employees. Employees are tasked with reporting suspicious emails and rewarded with positive automated feedback should their detection be accurate. Those who fail the spearphishing penetration test receive automated feedback on why they failed and what to look out for next time, again in a non-disruptive manner. This method becomes all the more effective when employees are aware of the training and that they are likely to receive test emails skills feedback at any given moment. The net effect is that employees are always on the look-out for suspicious emails and adopt a 'report-in-any-case' default position. This is a response promoted by the perception that an employee may fail the test and receive negative feedback, a reaction

108 See for example: (Mar. 29, 2018, 02:26 PM), https://cofense.com/; https://www.wombatsecurity.com/; and http://fissuresecurity.com/.

explained by fear appeal and protection motivation theory.[109] Nobody wants to fail a test and receive negative feedback, especially not high-conscientious and highly-competitive lawyers. Furthermore, with the overlay running on real work emails in addition to spearphishing test emails, employees are constantly having their skills of detection topped-up. Add to this the circulation of context-specific awareness material about various aspects of cyber security threats, and the likelihood of catching a real attempt at spearphishing increases dramatically.

The application of technology with respect to the overlay in this context is best described with reference to airline pilots' heads-up displays: "As the key source of information for pilots, the human visual system has necessarily driven much of the evolution in cockpit technology. In contrast to the complicated, gauge-based systems of the past, the electronic flight displays of today's modern airliners are testament to advances in human factors engineering. The next step in flight instrumentation, although already used for some 50 years in the military, is just beginning to emerge in civil transport aircraft. Head-up displays (HUD) allow pilots to see key flight instrumentation while viewing the outside world. The need to look down at the flight instruments is removed by the HUD, resulting in increased situational awareness and greater precision in aircraft control ...The primary flight displays of modern transport aircraft do an excellent job of presenting information to pilots in a way that promotes efficiency and good situational awareness. However, the need to transition from the use of head-down displays to outside visual reference at certain points in the flight continues to create an attentional division, often during critical management periods. The use of HUD brings primary flight management information and outside visual reference into the same visual scene, increasing the usefulness and relevance of displayed symbology".[110]

Training such as this, which helps employees identify aspects of an attack; gives them an opportunity to report suspicious emails; receive demonstrable feedback on their cyber defence competence level; and regularly tests for weaknesses in order to reinforce good cyber defence skills and awareness certainly holds promise for law firms. This is especially so because the training can be conducted consistently over any desired period of time or for as long as it takes for a clear improvement in cyber defence competence and behaviour and is done so on a non-disruptive basis and within lawyers' normal work environment. This, it is argued, circumvents the issues caused by law firm short-termism, such as the billable hour culture and 24/7 availability to clients, but also can bring a positive change to the issue of underregulation of law firm cyber security conduct. Firms that can demonstrate effective cyber defence of their personnel can use this to win new clients who have set requirements high for cyber security standards of their supply chain, and also bolster existing client relationships for the same reason.

---

109 Sebastian Schuetz, Paul Benjamin Lowry and Jason Thatcher, Defending Against Spear-Phishing: Motivating Users Through Fear Appeal Manipulations (June 27, 2016). 20th Pacific Asia Conference on Information Systems (PACIS 2016), Chiayi, Taiwan, June 27–July 1.

110 Nichol RJ (2015) Airline Head-Up Display Systems: Human Factors Considerations. Int J Econ Manag Sci 4: 248.

Training such as this, which helps employees identify aspects of an attack; gives them an opportunity to report suspicious emails; receive demonstrable feedback on their cyber defence competence level; and regularly tests for weaknesses in order to reinforce good cyber defence skills and awareness certainly holds promise for law firms. This is especially so because the training can be conducted consistently over any desired period of time or for as long as it takes for a clear improvement in cyber defence competence and behaviour and is done so on a non-disruptive basis and within lawyers' normal work environment. This, it is argued, circumvents the issues caused by law firm short-termism, such as the billable hour culture and 24/7 availability to clients, but also can bring a positive change to the issue of underregulation of law firm cyber security conduct. Firms that can demonstrate effective cyber defence of their personnel can use this to win new clients who have set requirements high for cyber security standards of their supply chain, and also bolster existing client relationships for the same reason.[111]

IV. CONCLUSION

As Wald notes, stopping all cyber attacks is impossible to do. Yet, 96% of hacking attacks employ simple techniques, and 97% of attacks can be blocked by common security practices that are within the reach of even small law firms and solo practitioners. Chief among these common cyber security practices is training employees to recognize deceptive attacks, known as spearphishing.[112] Law firms face unprecedented danger from cyber attack owing to the increase quantity, quality and diversity of attacks and attack sources, and are also more vulnerable to attacks, presenting a 'lower hanging fruit' to hackers, in terms of size of the prize (and therefore potential liability costs to law firms) vs. effort to break in, than organizations in other industries. While it is true that law firms need to do more to protect client information, the issue is far more complicated than first appears. Law firm cyber defence has been stymied by a mix of short-termism and underregulation of cyber security conduct, which manifests itself in the form of external factors, including lax regulatory standards and ethics rules as well as non-existent client pressure, and internal factors, such as the partnership model and PEP marker of success which is underpinned by the billable hour. We have outlined that as well as a recent spate of high-profile law firm data breaches, there is a regulatory shift is underway with the introduction of the GDPR and an incoming wave of future, similarly inspired measures around data protection in the Digital era and also a change in client attitudes toward protection of their confidential information, meaning that law firms are now under pressure to improve defences. We have made clear that while law firms traditionally have been unable to train employees to deal with spearphishing owing to the requirements of the billable hour and culture of 24/7 availability to clients, modern technological innovations hold the potential to update spearphishing training methodologies to both address and dramatically improve the

---

111 McNerney, Michael, and Emilian Papadopoulos. "Hacker's Delight: Law Firm Risk and Liability in the Cyber Age." American University Law Review 62, no.5 (2013): 1243-1272.

112 Ibid.

human behaviour aspect of cyber defence through skills and awareness development, and also be non-disruptive in-terms of delivery, allowing lawyers to stay in their normal work environment and maintain availability to clients. However, this is only one aspect of an effective cyber defence infrastructure. A collective effort is needed on behalf of all personnel within law firms – lawyers and non-lawyers, at every level of the hierarchy, to implement and manage a comprehensive governance framework that promotes good, proactive, cyber security practice that permeates the firm's culture. Effective training that caters for the human aspect of cyber defence by comprising behavioural science principles and which can be delivered within the present constraints of law firm short-termism and underregulation, coupled with the development, implementation and enforcement of effective cyber security policies and procedures are the first steps in establishing the foundational aspects of good cyber practices and defence competence. A culture of sustainable, incentive-aligned cyber security embedded into everyday practice, fit for the digital age law firm.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

SCOPE AND LIMITS OF THE GERMAN LEGAL SERVICES ACT FOR LEGAL TECH SERVICE PROVIDERS

Frank R. Remmertz

AUTHOR

Dr. Frank R. Remmertz is a certified lawyer for intellectual property and information technology law from Munich, Germany. He also specializes in legal profession law including the law regulating legal services in Germany. He is a member of the board of the Munich Bar Association and chairman of the committee "Legal Services" in the German Federal Chamber of Lawyers. He publishes legal essays in the field of IT law and the law regulating legal services on a regular basis, particularly pertaining to legal tech, and appears as guest speaker at conferences. He is, inter alia, co-author of a well-known commentary on the Legal Services Act (Krenzler, Rechtsdienstleistungsgesetz, 2nd ed. 2017).

ABSTRACT

In contrast to as in other jurisdictions, such as the United States or the UK, out-of-court legal services in Germany are strictly regulated by a statute, the Legal Services Act, which came into force nearly a decade ago and superseded the former Legal Counsel Act (Rechtsberatungsgesetz). According to this act, out-of-court legal services must be expressly permitted and are, in principle, reserved to lawyers. Consequently, there are certain legal restrictions for tech providers offering legal services in Germany that must be observed. The following article deals with the scope and limits for offering legal services by legal tech providers in Germany according to the German Legal Services Act. The author explains why some legal tech business solutions offering legal services may be in conflict with this act, which is a significant issue of compliance for both legal tech start-ups and their investors. Entrepreneurs, stakeholders of legal tech start-ups and capital investors should weigh the economic opportunities and legal risks carefully before placing a legal tech start-up on the German market.

TABLE OF CONTENTS

I. INTRODUCTION

Nothing is more constant than change.[1] This assertion by Heraclitus more than 2,500 years ago has never been truer – at least in the German legal market. The new phenomenon of legal tech has already brought about major changes in the market for legal services in recent years. And this is just the beginning. Traditionally, the concept of legal tech referred to the application of technology and software to help law firms make their office work easier and more efficient ("office tech"). In the past few years, a new dimension of legal tech has been emerging with technology start-ups disrupting the practice of law by giving clients access to online software that reduces and, in some cases, eliminates the need to consult a lawyer, or by connecting people with lawyers more efficiently with digital platforms and marketplaces, and lawyer-matching websites.[2] With no doubt, legal services are becoming more and more digitized.[3] This development is the result of a rapidly growing demand among many consumers for cost-effective and price-predictable "standardized" (or "commoditized") legal services rather than the costly "bespoke" legal solutions provided by lawyers.[4] Consumers are demanding more choice, transparency, price-predictability and direct access to providers.[5] According to the legal tech pioneer *Richard Susskind*,[6] the strongest drivers are the following: more-for-less-challenge,[7] liberalization and digitization. These drivers have resulted in a new kind of technology-based, consumer-oriented legal service provider and changed the legal market in the United States decades ago.[8] With a time lag, this trend has affected the German legal market as well. Germany's legal tech scene is said to be roughly 5 – 10 years behind the one in the United

1 HERACLITUS OF EPHESUS (Ἡράκλειτος, Herakleitos; c. 535 BC – 475 BC).

2 *Legal technology*, WIKIPEDIA (Mar. 29, 2018, 05:09 PM), https://en.wikipedia.org/wiki/Legal_technology.

3 Marc Cohen, *Legal delivery is becoming digitized. What does that mean?*, (May 21, 2017) FORBES (Mar. 29, 2018, 05:10 PM), https://www.forbes.com/sites/markcohen1/2017/05/21/legal-delivery-is-becoming-digitized-what-does-that-mean/#4bedc5914e62; see for the process of digital transformation in the German legal market: Zoë Andreae, *The Role of Legal Tech Startups in the Digital Transformation of the German Legal Industry*, ESADE BUSINESS SCHOOL, (Mar. 29, 2018, 05:13 PM), http://dd.lecare.com/legaltech.pdf; brief survey Zoë Andreae, *The Digital Transformation of the German Legal Industry*, LEGAL TECH BLOG (Mar. 29, 2018, 05:13 PM), http://legal-tech-blog.de/the-digital-transformation-of-the-german-legal-industry.

4 RICHARD SUSSKIND, TOMORROW'S LAWYERS, 23 et seq. (2013).

5 Marc Cohen, *Differentiation in the New Legal Marketplace and Why It Matters*, LEGALMOSAIC (Mar. 29, 2018, 05:18 PM), https://legalmosaic.com/2018/01/05/differentiation-in-the-new-legal-marketplace-and-why-it-matters/.

6 RICHARD SUSSKIND, TOMORROW'S LAWYERS, 23 et seq. (2013).

7 Richard Susskind, *A Response to the More for Less Dilemma*, 1, THE PRACTICE - HARVARD LAW SCHOOL, (Mar. 29, 2018, 05:20 PM), https://thepractice.law.harvard.edu/article/speakers-corner-richard-susskind/.

8 See for the history of digital legal services in the United States: Chris Johnson, *Leveraging Technology to Deliver Legal Services*, 23, HARVARD JOURNAL OF LAW AND TECHNOLOGY, 259, (Mar. 29, 2018, 05:20 PM), http://jolt.law.harvard.edu/articles/pdf/v23/23HarvJLTech259.pdf.

States but has more speed and dynamics.[9] This ongoing digital transformation of the German legal market is still a central driving force for change in the market. At a relatively early stage, in 2013, the DAV[10] predicted that, by 2030, standardized consulting services will be taken over by online providers and the internet will facilitate the process of lawyer referrals.[11] These assumptions have occurred much earlier than predicted. Last year, 2017, is considered the year with the most rapid growth in the legal tech market in Germany.[12] Many experts predict a disruption effect in the German legal service market making legal services more efficient, transparent, affordable and accessible.

However, there are certain legal restrictions for tech providers offering legal services in Germany that must be observed. In contrast to as in other jurisdictions, such as the United States or the UK, legal services are strictly regulated by a German statute titled the Legal Services Act (RDG).[13]

The following article deals with the scope and limits for offering legal services by legal tech providers in Germany according to the Legal Services Act,[14] a subject that is often neglected or even underestimated by many legal tech entrepreneurs. The article also provides an overview of recent developments in the law of legal services with respect to tech-enabled business models.

Last but not least, this subject is also a compliance issue for legal tech start-ups, its stakeholders and domestic and foreign capital investors,[15] business angels and financial institutions supporting new business models in the field of alternative legal services in Germany.[16]

---

9 Zoë Andreae, *Legal Tech Startups in Germany*, LEGAL TECH BLOG (Mar. 29, 2018, 05:24 PM), http://legal-tech-blog.de/legal-tech-startups-in-germany.

10 DAV = Deutscher Anwaltverein.

11 *The Legal Services Market 2030*, DEUTSCHER ANWALTS VEREIN (Mar. 29, 2018, 05:30 PM), https://anwaltverein.de/de/service/dav-zukunftsstudie.

12 *Legal Tech 2017: Ein Rückblick in 10 Punkten*, LEGAL TECH BLOG (Mar. 29, 2018, 05:32 PM), http://legal-tech-blog.de/legal-tech-2017-ein-rueckblick-in-10-punkten-teil-1; *Legal Tech 2017: Ein Rückblick in 10 Punkten (Teil 2)*, LEGAL TECH BLOG (Mar. 29, 2018, 05:32 PM), http://legal-tech-blog.de/legal-tech-2017-ein-rueckblick-in-10-punkten-teil-2.

13 RDG = Rechtsdienstleistungsgesetz.

14 See also Frank R. Remmertz & Nico Kuhlmann, *Legal Tech und das Rechtsdienstleistungsgesetz*, LEGAL TRIBUNE ONLINE (Mar. 29, 2018, 05:32 PM), https://www.lto.de/recht/legal-tech/l/legal-tech-rechtsdienstleistungsgesetz-legal-chatbots-vertragsgeneratoren/.

15 See for recent developments in the U.S. legal tech market: *Legal Tech Startup Financings Take Off As Automation Hits White-Collar Industries*, CBINSIGHTS (Mar. 29, 2018, 05:36 PM), https://www.cbinsights.com/research/legal-tech-funding-white-collar-automation/.

16 The number of venture-capital-based legal tech startups in 2016 compared to 2011 increased by a factor of 10 and is steadily rising, see Zoë Andreae, *Legal Tech Startups in Germany*, LEGAL TECH BLOG (Mar. 29, 2018, 05:24 PM), http://legal-tech-blog.de/legal-tech-startups-in-germany.

II. THE REGULATORY FRAMEWORK IN GERMANY

The legal services market in Germany has been regulated for many decades. In summer 2008, the Legal Services Act superseded the former Legal Counsel Act (Rechtsberatungsgesetz = RberG) of 1935.[17] The original aim of the Rechtsberatungsgesetz was to suspend Jewish people from offering legal services and to reserve this right to German advocates (Rechtsanwälte). This illegal and inhuman purpose was excluded by the legislative authorities after the 2nd World War but, in principle, the monopoly of lawyers to provide legal services has been upheld. Since the mid-90s, the statute has come more and more under criticism. It is no longer updated and both the Federal Supreme Court and the Federal Constitutional Court have made several corrections.[18] In the important judgment "MasterPat," the Federal Constitutional Court stated, inter alia, that the aim of the statute is to protect consumers rather than to guarantee a monopoly for lawyers. However, the court also upheld that the main principle of prohibition legal services with permission reservation is in the public interest.[19] This important principle was adopted in the Legal Services Act in 2008.

The German Legal Services Act regulates the legitimacy of legal services. The aim of the Act is to protect consumers, legal relations and the legal system against unqualified legal services (section 1 (1)). In this regard, it is important to note that the Legal Services Act is a consumer protection act, not an act to guarantee the monopoly of lawyers.[20] Despite pressure from EU institutions to deregulate the German legal market, the European Court of Justice held that the principle of prohibition legal services with permission reservation is justified in the public interest and therefore compatible with the freedom to provide services in the EU.[21] The Court of Justice held that the German legislation[22] is clearly intended to protect the recipients of the services in question against the harm they could suffer as a result of legal advice given to them by persons who did not possess the necessary professional or personal qualifications. This is justified in the public interest.[23] The same applies to the succeeding law, the Legal Services Act.

---

17 GESETZ ZUR VERHÜTUNG VON MIßBRÄUCHEN AUF DEM GEBIET DER RECHTSBERATUNG, December 13, 1935 (RGBl. I S. 1478, BGBl. III 303-12).

18 For more details, see Frank Remmertz, *in* Rechtsdienstleistungsgesetz, § 1 note 1 (Michael Krenzler, 2nd ed. 2017).

19 Federal Constitutional Court (= BVerfG); BVERFG JUDGMENT OF OCTOBER 29, 1997 – 1 BvR 780/87, BVerfGE 97, 12, 26ff. = NJW 1998, 3481 (MasterPat).

20 As stated in section 2 of the UKlaG (Unterlassungsklagengesetz); see Frank Remmertz, *in* Rechtsdienstleistungsgesetz, § 1 note 68 (Michael Krenzler, 2nd ed. 2017).

21 See COURT OF JUSTICE, Judgment of July 25, 1991 – C-76/90 – Säger ./. Dennemeyer & Co. Ltd, with respect to the former RBerG.

22 With respect to the former RBerG.

23 COURT OF JUSTICE, Judgment of July 25, 1991 – C-76/90, notes 16, 17; this statement has been confirmed by the COURT OF JUSTICE in its judgment of December 17, 2015 – C-342/14 – X-Steuerberatungsgesellschaft ./. Finanzamt Hannover-Nord, note 53 and the case-law cited.

III. COMPARATIVE LEGAL OVERVIEW

In Europe, the law regulating legal services is handled differently depending, inter alia, on the membership of each country in the common law or civil law legal system.[24] In some countries, the legal restrictions for offering legal services are less strict than in Germany. Especially in the UK,[25] for out-of-court legal services, there is no monopoly for lawyers and the market has been more liberalized by the UK Legal Services Act 2007 introducing ABS ("Alternative Business Structure") enabling non-lawyers to own and run the company.[26] It is allowed for outside investors from private equity or venture capital to invest in an ABS and become a partner of the firm. ABSs allow businesses other than law firms to offer legal services. This development is a contrast to the more conservative regulation in Germany, which still strictly prohibits foreign capital in law firms.

In this context, it is worth noting that although the legal situation in some EU member states is less strict than in Germany, this is compatible with EU law, particularly with the freedom to provide services in the EU. As the Court of Justice stated, the fact that some member states impose less strict rules than other member states does not mean that the latter's rules are disproportionate and hence incompatible with EU law.[27] In the absence of specific Community rules, each member state is free to regulate the exercise of legal services in its territory.[28]

IV. THE SCOPE OF THE LEGAL SERVICES ACT 2008

A. General remarks

The Act only governs out-of-court legal services such as legal advice and legal representation of clients in out-of-court disputes and before public authorities. Legal representation before a court is regulated by other specific rules of procedure and – save in exceptional cases – reserved for lawyers. Therefore, legal tech service providers must observe the Legal Services Act when they offer out-of-court legal services. Litigation services are not permitted for them.

In principle, all legal services must be performed exclusively by either (a) lawyers or (b) non-lawyers explicitly permitted by law to provide legal services (section 3). In other

---

24 An overview is given in the explanatory memorandum for the Legal Services Act: BT-Drs. 16/3655, 28 et seq.

25 The landscape of legal tech start-ups is illustrated on (Mar. 29, 2018, 05:47 PM), https://www.legalgeek.co/startup-map/.

26 See also Crispin Passmore, *What is happening to the regulation of the legal market in England and Wales?*, ANWALTSBLATT, 140 (2014) et seq.; Joanna Goodman, *The UK legal tech scene, in* Legal Tech – Die Digitalisierung des Rechtsmarkts 67 (Markus Hartung, Micha-Manuel Bues, Gernot Halbleib et al eds., 1st ed. 2018).

27 COURT OF JUSTICE, judgment of December 12, 1996 – C-3/95 – note 42 – Broede vs. Sandker, with respect to the former RBerG.

28 COURT OF JUSTICE, judgment of December 12, 1996 – C-3/95 – note 37 – Broede vs. Sandker.

words: A legal service provider must either be a fully qualified lawyer or another person with the legal authority to do so. This legal authorization may be either stipulated in the Act itself or regulated elsewhere by law (section 3). For example, tax advisors may provide legal tax services based on the Tax Consultancy Act.

An important permission to provide legal services in the Act itself is regulated in section 5, which allows legal services as complementary services. The legal services must then be provided in connection with another non-legal activity. Examples are legal advice provided as a supplementary service by consultants, tax advisors or accountants. For legal tech solutions offering legal services as the key or main business, this statutory permission in section 5 is not an option.

According to the Legal Services Act, legal services may also be provided by a "registered person." According to section 2 (2), regardless of whether the service fulfils the definition of "legal services" in section 1, the collection of third-party claims is a legal service if the debt collection is conducted as a stand-alone business (collection service). In the legal tech market in Germany, registered providers for collection services according to section 2 (2) are of significant relevance. In fact, many legal tech providers are registered as collection service providers enabling them to pursue outstanding debts including compensation claims on behalf of their clients. However, the permission is restricted to monetary claims. Other claims such as the cancellation of an agreement or the defense against claims do not fall within the scope of "collection services."

B. Territorial scope

The territorial scope of the Legal Services Act has been modified due to a recent legal reform in 2017.[29] For legal tech service providers acting from outside of Germany, section 1 (2) of the Act stipulates the following: "Where a legal service is provided exclusively from another state, this Act only applies where its subject matter is German law." Therefore, if legal tech service providers are offering their services via the internet across the border, the Act only applies if legal advice is given / legal services are offered in German law.[30] This applies, in principle, irrespectively of whether the foreign state is a member of the European Union or not (such as the United States).

If legal tech service providers situated in an EU member state[31] are offering digital services via the internet to German consumers, it is controversial as to whether they can benefit

29 GESETZ ZUR UMSETZUNG DER BERUFSANERKENNUNGSRICHTLINIE UND ZUR ÄNDERUNG WEITERER VORSCHRIFTEN IM BEREICH DER RECHTSBERATENDEN BERUFE v. 12.5.2017, BGBl. I, 1121, 1143.

30 For further details see Frank Remmertz, *in* Rechtsdienstleistungsgesetz, § 1 note 81 (Michael Krenzler, 2nd ed. 2017).

31 The e-commerce directive is not applicable for U.S. legal tech companies. After the Brexit, UK may also be regarded as a third-party state.

from the privileges granted by the e-commerce directive,[32] particularly if the directive also applies to legal services by replacing the principle of prohibition in the German Legal Services Act. According to the e-commerce directive, the law of the country of origin applies if the services are provided exclusively by electronic means. However, the recitals and the interpretation of the directive as well as the implementing German Telemedia Act indicate that, for legal services, the laws of the country of destination (such as Germany) shall prevail.[33] Otherwise, any economic activity could theoretically fall within the scope of the directive 2000/31/EC because all traders and service providers are able to offer services by electronic means.[34] Therefore, there are good reasons for why the privileges granted by the e-commerce directive apply to the means of electronic communication and not to services as such. Furthermore, the e-commerce directive allows that member states may take measures that are necessary to protect consumers (Art. 3, section 4a of directive 2000/31/EC).[35] The German Legal Services Act is such a legislative measure to protect consumers against unqualified legal service providers. The Court of Justice stressed that the protection of consumers is an objective that may be regarded as an overriding reason in the public interest capable of justifying a restriction of the freedom to provide services.[36] Consequently, legal services are not per se privileged only because they are offered by electronic means. Therefore, if legal tech service providers are offering their services from abroad via electronic means to German consumers, the Act applies when its subject matter is German law (section 1 (2) of the Legal Services Act).

C The definition of "legal services"

The Legal Services Act is only applicable if a service can be regarded as a "legal service" according to the definition in section 2 (1) of the Act. This is always the key question when applicability of the Act is concerned and plays a major role for legal tech service providers in assessing whether their service is permitted or not. According to section 2 (1) of the Act, a "legal service" is defined as "any service provided to a third person that requires a legal assessment of the particular case." The "legal assessment" must reach a certain threshold: Every matter requires a legal assessment of the individual case if it goes beyond the purely schematic application of the law. A legal assessment does not cover a sole repetition or schematic application of legal reading. However, according to established case law of the Federal Supreme Court (BGH), there is only a low level for the assumption of a "legal

32 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce).

33 For further details see Frank Remmertz, *in* Rechtsdienstleistungsgesetz, § 1 note 98 (Michael Krenzler, 2nd ed. 2017).

34 See Opinion of Advocate General Szpunar of May 12, 2017, C-434/15 – Asociatión Profesional Elite Taxi ./. Uber Systems Spain SL, note 87.

35 FEDERAL SUPREME COURT, Judgment of October 5, 2006 – I ZR 7/04 – note 13 – Schulden-Hulp.

36 COURT OF JUSTICE, Judgment of December 17, 2015 – C-342/14 – X-Steuerberatungsgesellschaft ./. Finanzamt Hannover-Nord, note 53 and the case-law cited.

assessment."[37] It does not matter if the rights issues are simple or difficult. Therefore, even when the legal matter is simple and can be standardized and automated on digital platforms, the low level of a "legal assessment" can be achieved. For tech-enabled legal services, it is important to note that there is only a low level of the threshold to fulfill the requirements of the definition of a "legal service" specified in section 2 (1) of the act.

On the other hand, general information given about the law on the internet is not covered by the definition and therefore allowed. Furthermore, the mere connection between consumers and lawyers via legal tech platforms or the referral to / recommendation of a specific lawyer does not fulfil the requirements of a legal service.

D Further requirements according to the Act

According to the Legal Services Act, there are further requirements that should be observed. Firstly, the legal tech company offering legal services must in itself be qualified to provide legal services. It is neither sufficient if the managing director of the company is qualified as a lawyer[38] nor if the company has employed lawyers who do the legal work. Secondly, the prohibition cannot be eluded if a legal tech company instructs independent lawyers as subcontractors. The subcontractors must then be regarded as servants of the company.[39] If the company itself is not qualified and permitted to provide legal services, the services are forbidden.

V. CLASSIFICATION OF LEGAL BUSINESS MODELS

In Germany, there are different categories and types of legal tech service providers.[40]

In a study conducted by the Boston Consulting Group and the Bucerius Law School, Germany,[41] the legal tech business models were categorized into 3 general groups: "enabler

37 FEDERAL SUPREME COURT, Judgment of January 14, 2016 – I ZR 107/14 – Schadensregulierung durch Versicherungsmakler, note 43; Judgment of March 31, 2016 – I ZR 88/15 – Rechtsberatung durch Entwicklungsingenieur, note 23.

38 FEDERAL SUPREME COURT, Judgment of February 22, 2005 – XI ZR 41/04.

39 FEDERAL SUPREME COURT, Judgment of July 29, 2009 – I ZR 166/06 – Finanz-Sanierung.

40 Zoë Andreae, *Legal Tech Startups in Germany*, LEGAL TECH BLOG (Mar. 29, 2018, 05:24 PM), http://legal-tech-blog.de/legal-tech-startups-in-germany; A list of companies can be found on (Mar. 29, 2018, 05:55 PM), http://tobschall.de/legaltech/. A landscape of the German legal tech scene is illustrated by Dominik Tobschall, *German Legal Tech Overview* (Mar. 29, 2018, 05:55 PM), http://tobschall.de/2016/06/25/german-legaltech-overview/; An international overview is published on (Mar. 29, 2018, 05:58 PM), https://techindex.law.stanford.edu/ (Stanford CodeX, the Stanford University Center for Legal Informatics).

41 Christian Veith, Michael Wenzler, Markus Hartung et. al., *How Legal Technology Will Change the Business of Law*, FINAL REPORT OF BUCERIUS LAW SCHOOL AND THE BOSTON CONSULTING GROUP ON IMPACTS OF INNOVATIVE TECHNOLOGY IN THE LEGAL SECTOR, (Mar. 29, 2018, 05:58 PM), http://www.bucerius-education.de/fileadmin/content/pdf/studies_publications/Legal_Tech_Report_2016.pdf.

technologies facilitating the digitization of legal data (1), support-process-solutions infusing new efficiencies into case management and back-office work (2), and substantive law solutions supporting or replacing lawyers in executing core legal tasks in transactions and litigation cases"[42] (3). The third category contains several subcategories.[43] A similar study was conducted in 2015 by Professor Oliver R. Goodenough[44] who divides the legal tech landscape into 1.0, 2.0 (which can be compared to category 3) and 3.0 stages. Today, we are rapidly approaching the 3.0 level including the implementation of smart contracts, artificial intelligence and machine learning.[45]

VI. CONFLICT WITH THE LEGAL SERVICES ACT

Particularly the category (3) – replacing (traditional) lawyers in providing legal advice and services – can be in conflict with the German Legal Services Act.

Traditionally, giving legal advice or representing clients in legal cases fully complies with the requirements of the definition of "legal services" in section 2 (1) of the Legal Services Act. It does not matter if the legal advice is given personally, by telephone, e-mail or via the internet by using a software. Therefore, the requirements of the definition of "legal services" can be fulfilled if the legal advice or legal assessment of a legal case is the result of a software. Using a software is only a technical tool enabling the provider to offer the legal service. According to the explanatory memorandum of section 2 of the Legal Services Act, it is irrelevant if the legal service is provided with technical assistance (and which) or not.[46] Software must be regarded as technical assistance for providing legal services. Hence, a software enabling the consumer to find the right legal solution by using a question-and-answer tool must be regarded as a legal service provided by the person offering these services. The sometimes heard objection that the developer (provider) of the software cannot be responsible for usage by the consumer is not convincing because the result of the usage is the result of the programming of the software.[47] In this context, legal chatbots will become relevant. Legal chatbots[48] are text-based dialog systems characterized by a question-

42 See footnote 44, page 4 and 5.

43 See footnote 44, page 5.

44 Oliver R. Goodenough, *Legal Technology 3.0*, HUFFPOST (Mar. 29, 2018, 05:59 PM), https://www.huffingtonpost.com/oliver-r-goodenough/legal-technology-30_b_6603658.html.

45 See Ron Friedman with critical remarks: *Bots, Big Data, Blockchain, and AI – Disruption or incremental change?*, BUCERIUS EXECUTIVE EDUCATION (Mar. 29, 2018, 06:08 PM), http://www.bucerius-education.de/home/news-termine/blog/article/bots-big-data-blockchain-and-ai-disruption-or-incremental-change/.

46 Explanatory memorandum for the Legal Services Act: BT-Drs. 16/3655, 47 et seq.

47 FEDERAL SUPREME COURT, Judgment of May 14, 2013 – VI ZR 269/12 – Autocomplete, note 17, with regard to the autocomplete function of Google.

48 Nico Kuhlmann, *Legal Chatbots – The next frontier of transformation in law*, LEGAL TECH BLOG (Mar. 29, 2018, 06:09 PM), http://legal-tech-blog.de/legal-chatbots-the-next-frontier-of-digital-transformation-in-law;

and-answer session incorporated in a software and resulting in concrete legal advice, a legal document or another specific legal service. All these services may be regarded as legal services within the meaning of the Act if the (low) level of threshold for legal examination is reached.

Furthermore, companies offering tech-enabled, easily accessible, user-friendly and low-cost access to legal documents and contracts with standardized legal texts can also conflict with the Legal Services Act if individualized documents or contracts are the result of a tech-enabled interaction between service provider and client that meets the needs of the client in his/her individual case. These services must also be regarded as legal services because it is irrelevant if, for example, a will, a managing contract or a purchase agreement is drafted by a lawyer or generated by a software.

Currently, it is controversial whether legal process outsourcing models offering legal services to lawyers, tax consultants or in-house lawyers etc. are compatible with the Legal Services Act, i.e. if an external service provider offers the drafting of written submissions, contracts or other legal documents to lawyers. Although the service definitely fulfils the requirement of the definition of a "legal service" pursuant to section 2 (1), it is doubtful if the addressee of the legal service, a lawyer or a tax consultant, must be "protected" in the same way as other consumers against unqualified legal services according to section 1 (1) of the Act.[49] Also, if legal services are to be provided to non-lawyers, the activity must be restricted to support services. For example, the Federal Constitutional Court[50] decided in 1997 that the surveillance of patent annuity fees does not require the full qualification of patent attorneys or lawyers and can also be provided by private firms. Therefore, legal services going beyond comparable support services are not permitted if they are offered by private firms. This result has been confirmed by the Federal Supreme Court.[51] The court decided that the application of intellectual property rights (trademarks, designs or patents) requires the qualification of a lawyer or patent attorney and cannot be outsourced and provided by non-lawyers. The same must apply to other legal documents such as contracts and written submissions.

Many legal tech companies are specialized in the examination and procurement of outstanding claims such as compensation claims.[52] In order to obtain a permission to provide

---

Robert Ambrogi, *This Week In Legal Tech: Everyone's Talking About Chatbots*, ABOVE THE LAW (Mar. 29, 2018, 06:11 PM), https://abovethelaw.com/2017/04/this-week-in-legal-tech-everyones-talking-about-chatbots/.

49 For further details see Frank Remmertz, *in* Rechtsdienstleistungsgesetz, § 1 note 68 (Michael Krenzler, 2nd ed. 2017).

50 FEDERAL CONSTITUTIONAL COURT (=BVerfG), BVerfG, decision of October 29, 1997 – 1 BvR 780/87, BVerfGE 97, 12, 26ff. = NJW 1998, 3481 (MasterPat).

51 FEDERAL SUPREME COURT, Judgment of March 31, 2016 – I ZR 88/15 – Rechtsberatung durch Entwicklungsingenieur.

52 A prominent example is "flightright," see (Mar. 29, 2018, 06:16 PM) https://www.flightright.co.uk/.

legal services, a significant part of them obtained registration according to section 2 (2) of the Act (collection services). As a registered legal service provider, they are also allowed to give legal advice connected with the collection services.[53] However, the collection services must be restricted to monetary claims. It is not allowed to pursue other claims such as the defense of third-party claims or the revocation of an agreement.

In principle, legal platform business models connecting clients to lawyers do not conflict with the Legal Services Act. The placement or recommendation of lawyers is not a legal service within the meaning of section 2 (1) of the Act. However, legal platform providers cooperating closely with external lawyers can be in conflict due to the above-mentioned[54] rule that a lawyer may not act as subcontractor for the service provider. Even if there will formally be a separate mandate between client and lawyer, the lawyer may be regarded as a sole subcontractor if the service provider controls the instruction and procedure of the mandate.[55]

IV. CONCLUSION AND OUTLOOK

In summary, legal tech business solutions offering legal services may be in conflict with the German Legal Services Act if they provide "legal services" within the meaning of section 2 (1) of the Act. The simple fact that legal services can be automated and provided with the support of a software cannot justify another conclusion. The consumer must also be protected against unqualified automated, tech-enabled legal services, i.e. wrong software results or untrustworthy legal tech providers, in the same way as against unqualified traditional legal services. In this context, it is important to note that, under current German law, non-lawyers offering legal services are neither obliged to have a professional liability insurance nor subject to professional rules such as the duty to observe professional secrecy and to avoid representing conflicting interests.

Legal solutions based on AI (Artificial Intelligence) and the use of self-executing contracts (smart contracts) will most likely be enabled in the near future.[56] Due to the nature of blockchain technology and its reliance on transparency and security for content, the significance of blockchain technology in the legal sector will probably increase significantly.[57]

---

53 FEDERAL CONSTITUTIONAL COURT, Judgment of February 20, 2002, 1 BvR 423/99 – Inkasso I, note 31.

54 See Chapter VI. D. (above).

55 FEDERAL SUPREME COURT, Judgment of July 29, 2009 – I ZR 166/06 – Finanz-Sanierung.

56 Christian Veith, Michael Wenzler, Markus Hartung et. al., *How Legal Technology Will Change the Business of Law*, FINAL REPORT OF BUCERIUS LAW SCHOOL AND THE BOSTON CONSULTING GROUP ON IMPACTS OF INNOVATIVE TECHNOLOGY IN THE LEGAL SECTOR (Mar. 29, 2018, 05:58 PM), http://www.bucerius-education.de/fileadmin/content/pdf/studies_publications/Legal_Tech_Report_2016.pdf.

57 See recently Kayla Matthews, *Blockchain and How It Will Benefit the Legal Industry*, LAW TECHNOLOGY TODAY (Mar. 29, 2018, 06:21 PM), http://www.lawtechnologytoday.org/2018/02/blockchain-and-how-it-will-benefit-the-legal-industry/; Jasmine Ye Han, *How Blockchain technology is transforming the legal industry*, BIG LAW BUSINESS (Mar. 29, 2018, 06:19 PM), https://biglawbusiness.com/how-blockchain-technology-is-

Like tech-enabled contract drafting (Vertragsgeneratoren), offering self-executing contracts in individual cases based on blockchain technology (smart contracts) also requires permission according to the Legal Services Act. From a legal standpoint, there is no difference between providing contracts by a lawyer and automated contract drafting.

Last but not least, the permission to provide legal services under the German Legal Services Act is a significant issue of compliance: Entrepreneurs, stakeholders of legal tech start-ups and capital investors should weigh the economic opportunities and legal risks carefully before placing a legal tech start-up on the German market. Offering legal services without permission must be regarded as an illegal commercial practice according to the Act Against Unfair Competition. As a result, competitors and certain associations may file injunctions and sue for damages.

Irrespective of the undoubted advantages of legal tech service models, especially the ability to enable consumers to pursue low-budget claims against big companies (access to justice), it seems necessary to regulate the legal tech market, either on the national level by implementing a permission clause in the Legal Services Act or on the European level. The EU Commission made it clear that digital platforms will be promoted but the rights of consumers must also be protected.[58] Regulation would also lead to legal security with advantages for investments for both legal tech start-ups and their investors.

transforming-the-legal-industry/; an example of a transfer agreement based on blockchain technology is illustrated by Dean Sonderegger, *Blockchain: Can Smart Contracts Replace Lawyers?*, ABOVE THE LAW (Mar. 29, 2018, 06:22 PM), https://abovethelaw.com/2018/02/blockchain-can-smart-contracts-replace-lawyers/.

58 "Online Platforms and the Digital Single Market – Opportunities and Challenges for Europe," Communication from the EU Commission COM (2016) 288 final (Mar. 29, 2018, 06:23 PM), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0288&from=EN.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

REPORT ON SPECIALIST SCIENTIFIC CONFERENCE "COMPLIANCE MANAGEMENT IN INSTITUTIONS OF THE HEALTHCARE SYSTEM" ON MARCH 9, 2018 IN BIELEFELD

Dr. Martina Orrù

AUTHOR

Martina Orrù works as scientific associate in the Office for Expert Opinions and Criminal Defense of Prof. Dr. Hendrik Schneider in Wiesbaden (Germany). In 2017, she acquired the Doctor title in law by a Co-Tutelle de Thesis between the Università degli Studi di Cagliari (Italy) and the Goethe University of Frankfurt am Main. Since 2015, she has been licensed as an attorney-at-law (Avvocato) in Italy and since 2018 she has been operating in Germany.

The insufficient entry of the registered doctors by the criminal offense elements of the German Criminal Code, which serve the protection against corruption, caused a significant reform of the 26th Section of the German Criminal Code in 2016. With the entry into force of Sections 299a and b Criminal Code (corruption and bribery in the healthcare system) the doors of the Healthcare Compliance have been opened. The topic is still relatively new and unexplored, however, several focuses can be identified already, which were discussed at this conference.

Bielefeld is distinguished in the Healthcare Compliance field by the research center Bielefeld Center for Healthcare Compliance (BCHC) under the management of Professor Dr. Michael Lindemann, professor for criminal law, criminal procedural law and criminology at the University of Bielefeld, as well as co-publisher of an important magazine in the German language relating to medical criminal law (medstra). The Bielefeld Center for Healthcare Compliance (http://www.jura.uni-bielefeld.de/lehrstuehle/lindemann/bchc) concerns a non-commercial university institution, which researches theoretical and practical questions of Healthcare Compliance in an interdisciplinary context.

An important exchange of opinions took place on March 9, 2018 at the University of Bielefeld with the specialist scientific conference "Compliance Management in Institutions of the Healthcare System", which was organized by the BCHC in cooperation with the working group medical law of the German Lawyers' Association [Deutscher Anwaltsverein]. The Compliance questions were in particular presented from the point of view of criminal law, criminology and labor law. The speakers (besides Professor Lindemann: attorney-at-law Dr. Maximilian Warntjen, Berlin, attorney-at-law Dr. Matthias Dann, Düsseldorf, attorney-at-law Dr. Rudolf Ratzel from Munich and Prof. Dr. Oliver Ricken, University of Bielefeld) involve experts in the field of German law. International references were only established marginally by this selection of the group of speakers. The following knowledge was discussed as a summary:

Various studies[1] have examined the distribution and effectiveness of Compliance Management systems in the healthcare system[2]. After the entry into force of the criminal offense elements relating to the prevention of corruption in the healthcare system in 2016 in the German Criminal Code, the attention paid to Compliance questions in the sanitary working environment has increased substantially. In the opinion of the speakers, however, the effectiveness of the internal company systems for the prevention of Compliance incidents is still insufficient. Under this aspect criminology can make a contribution. The

---

1 Prof. Dr. H. Schneider, Dr. jur. K. Grau & Dipl. Soz. K Kißling, *The shock of Berlin hit deep! – Results of an empirical research project relating to Compliance in the healthcare system and the pharmaceutical industry*, 2, CORPORATE COMPLIANCE ZEITSCHRIFT 48 et seqq. (2013), shows that 2011-2012 only 28.3% of those questioned in the healthcare system and 76% of those questioned in pharmaceutical industries have written Compliance regulations. According to the study "Compliance on the clinic market" (2017) 83.8% of the questioned hospitals have a Compliance Management System, http://www.ey.com/Publication/vwLUAssets/EY_-_Compliance_im_Klinikmarkt/$FILE/ey- compliance-im-klinikmarkt.pdf.

2 The following presentation refers to the lectures and the presentations of the speakers.

efficiency of a Compliance Management Systems is to be fully linked with the corporate culture and its aims. The Compliance debate is thus to be connected with the discussion about business ethics, for which, in the opinion of the speaker, criminology is also responsible. The ethic components were neglected so far owing to a focus on the legal questions. The Compliance System can be compared to a house, with which the foundation walls consisted of ethical guidelines and values[3].

Whether Compliance Guidelines are effective as a means of conduct control within the scope of the prevention of corruption, cannot be examined empirically yet owing to the circumstance that the relevant German criminal laws have only been in force since 2016. The central task of the prevention by Compliance Management is, however, to clarify under which prerequisites fees for the conducting of clinical trials, invitations of the industry to further training or further training trips, or cooperation contracts between clinics and doctors operating in the outpatient sector (procurement of clinic patients by the doctor operating in the outpatient sector against financial advantages) are possible still. There are no doubts that with such complex legal questions the Compliance Management will place an important role. The development of approval or examination procedures is of central importance before the doctor enters into a cooperation with the industry. Further decisive is the quality of the information provided to the standard addresses (employees). Criminal offences are committed, because the subtle limits between permitted cooperation and corruption are not always known. Therefore, it is necessary to teach and train employees accordingly by Compliance programs.

Special attention was further paid to the topic of the "panel doctor" (according to German law this concerns a doctor, who treats patients, who have a statutory health insurance) and his remuneration. The German settlement system is susceptible for manipulations and settlement fraud. The analysis of this phenomenon requires a differentiated analysis, depending on whether it concerns the settlement of an outpatient service in the doctor's practice or an inpatient service in the hospital. On the other hand, Compliance risks and favorable opportunities for an offence to be committed arise in the system of German healthcare owing to the lack of transparency and the complexity of the statutory regulations. As these make a distinction between the insurance status of the patient and the place where the service is provided (practice or hospital). A patient with statutory health insurance does not receive any settlement of the treatment in the German healthcare system (no "bill") so that settlement manipulations, for example the settlement of services that were not provided, are not recognizable for him.

Finally, aspects under labor law are to be taken into consideration in the Compliance organization. Significant in the field of the effectiveness of the Compliance Management System is the topic of "whistleblowing". After all, this concerns the only element in the system that envisages a "bottom up" communication. In Germany, there is no general obligation to report criminal offences. The protection of the person giving an indication is

3 Cf. with regard to these aspects also Daniela Dietzfelbinger, *Integrity Culture as a Forward-Looking Success Factor: A Practical Example*, 3, COMPLIANCE ELLIANCE JOURNAL, 53 et seqq. (2017).

not yet sufficiently provided for either. Furthermore, reporting obligations by whistleblower regulations for company employees should be discussed. These are currently at the most envisaged by regulations in the employment contract (for example for Compliance Officers), however not by law.

The food for thought offered by the conference is numerous and productive. The penetration between science and practice, which made substantial progress, is additionally successful.

A comparison of the discussion about Healthcare Compliance with the international position of research is useful beyond the topic of the conference. Germany should not, however, be representative for Europe either. In Italy, Pandora's Box has not even been opened yet. The gradually beginning discussion is deemed equivalent to breaking a taboo, because the topic has been concealed under a veil of silence so far.